Álgebra Diferencial aplicada a la búsqueda de condiciones necesarias para la existencia de Antiderivadas Elementales

Rafael Eduardo Francois Dubois Pappa

UNIVERSIDAD DEL VALLE DE GUATEMALA

UNIVERSIDAD DEL VALLE DE GUATEMALA
Facultad de Ciencias y Humanidades

Álgebra Diferencial aplicada a la búsqueda de condiciones necesarias para la existencia de Antiderivadas Elementales

Trabajo de graduación en modalidad de tesis presentado por
Rafael Eduardo Francois Dubois Pappa
para optar al grado académico de Licenciado en Matemática Aplicada

Guatemala,
2024

UNIVERSIDAD DEL VALLE DE GUATEMALA
Facultad de Ciencias y Humanidades

Álgebra Diferencial aplicada a la búsqueda de condiciones necesarias para la existencia de Antiderivadas Elementales

Trabajo de graduación en modalidad de tesis presentado por
Rafael Eduardo Francois Dubois Pappa
para optar al grado académico de Licenciado en Matemática Aplicada

Guatemala,
2024

Vo.Bo.:

(f) ______________________________
Lic. Monica Lucía Cabria Zambrano

Tribunal Examinador:

(f) ______________________________
Lic. Monica Lucía Cabria Zambrano

(f) ______________________________
MSc. Alan Gerardo Reyes Figueroa

(f) ______________________________
MSc. Dorval José Manuel Carias Samayoa

Fecha de aprobación: Guatemala, 5 de enero de 2024.

Prefacio

La motivación detrás de este estudio surgió del interés en un resultado que suele ser citado pero nunca demostrado en muchos cursos introductorios de cálculo: la inexistencia de *antiderivadas elementales* para ciertas funciones que en primera inspección no poseen ninguna peculiaridad.

Incluso antes de entrar a la universidad, la integración y las técnicas asociadas a la solución de integrales me despertaron un gran interés. Entrando de lleno al estudio del cálculo, pude apreciar la aplicabilidad y la utilidad de las antiderivadas como funciones que surgen en soluciones a problemas de física, estadística, economía, entre otras disciplinas. Desde entonces, he tenido la oportunidad de estudiar y notar varios patrones que resultan casi algorítmicos en la solución de muchas integrales, así como he podido encontrar funciones importantes que provienen de integrandos cuya antiderivada no es elemental. Por ejemplo, la función de distribución probabilística de una distribución normal. El misterio alrededor de estas funciones me pareció casi místico por mucho tiempo, y siempre quise entender la razón detrás de la inexistencia de sus antiderivadas.

Durante la licenciatura se estudia el Análisis de Variable Real, un curso en el cual un resultado importante es que toda función continua definida en un intervalo es integrable en el sentido de Riemann. Fue evidente, desde entonces, que el problema de encontrar una antiderivada elemental no es un problema que pueda resolverse dentro del cálculo. Poco después, en un curso que se concentró en teoría de Galois, pude presenciar el procedimiento detrás de la demostración del teorema de imposibilidad de Abel. Dicho teorema afirma la inexistencia de una fórmula general para encontrar los ceros de un polinomio de grado mayor a 4 a través de sus coeficientes, utilizando únicamente operaciones de campos y radicales. Fue aquí que noté un paralelo con el problema de la integración indefinida, pues ambos estudian la incapacidad de representar de manera algebraica a objetos que existen dentro del análisis. Esto me llevó a investigar más sobre el tema, leyendo un poco sobre Teoría Diferencial de Galois. Aunque dicha teoría va más allá de lo que se discute en la presente tesis, fue el interés en la misma el que me llevó a descubrir sobre el Principio de Liouville, los métodos de Rothstein y Trager, los algoritmos de integración de Risch, y muchas otras herramientas utilizadas en este trabajo investigativo. Mi viaje a través de estas ramas de la matemática ha sido una aventura que he disfrutado verdaderamente, y es por ello que quise compartir y ahondar en lo que he aprendido a través de esta investigación.

Agradecimientos

El desarrollo de este trabajo de graduación no hubiera sido posible sin todos los aprendizajes que pude adquirir dentro de la Universidad del Valle de Guatemala, y el cuerpo docente que me acompañó a lo largo de estos cinco años de licenciatura. Agradezco profundamente sus enseñanzas y paciencia, así como la vocación y el amor que compartimos todos por la matemática y su belleza.

Agradezco también a mi familia y amigos, quienes siempre han estado a mi lado y han aportado grandemente a mi educación desde una edad temprana. A mi familia, por su cariño y por darme el privilegio de estudiar lo que más me gusta. Y a mis amigos, por ser quienes lograron sacarme de las situaciones estresantes que la vida pudo poner en mi camino. Especialmente agradezco a mis compañeros de aprendizaje en la matemática, tanto quienes me acompañaron a divertirme resolviendo problemas y demostrando teoremas (algunos incluso desde las Olimpiadas de Matemática en la secundaria), como quienes simplemente estuvieron a mi lado durante la carrera.

Me parece necesario extender un agradecimiento especial a mis amigos de Capella Cantorum y de Cafella. Con ellos me he desarrollado artísticamente, he cantado y me he adentrado cada vez más a la música coral, lo cual ha sido un aporte realmente significativo a mi vida. No sé si mi carrera universitaria hubiera sido lo mismo sin las experiencias que he vivido a su lado, y espero que nos sea posible continuar haciendo música juntos.

No puede faltar un agradecimiento simbólico a las mascotas que me han acompañado a lo largo de mi vida, quienes me han dado el amor más incondicional que alguna vez he conocido. Gracias por tanto cariño a May, Nina y Marnie, estoy seguro de que hicieron de mi vida académica un camino más fácil de recorrer.

Índice

Resumen

En la presente tesis se definen a los operadores diferenciales en el contexto del álgebra, de manera que la antiderivada pueda ser vista como un operador inverso entre campos diferenciales. Se examinan a las funciones elementales como objetos algebraicos que presentan propiedades diferenciales especiales, con el objetivo de determinar las condiciones necesarias para que la antiderivada de una función sea elemental. Con esto en mente, se presenta un algoritmo de integración de funciones racionales que representa a la integral a través de una parte racional y una parte logarítmica, haciendo uso del resultante de Sylvester como herramienta. Este resultado se generaliza para cualquier campo de funciones elementales, de manera que si una antiderivada es elemental, entonces debe poseer una parte dentro de dicho campo, adicional a una parte compuesta por una cantidad finita de logaritmos de funciones en ese campo. Finalmente, se presentan algoritmos de Risch para integración de funciones elementales trascendentales, los cuales determinan si una función en campos con extensiones logarítmicas y exponenciales posee una antiderivada elemental, y en caso afirmativo, se presenta la solución en términos de una cantidad finita de funciones elementales.

CAPÍTULO 1

Introducción

En la matemática, la habilidad de encontrar la antiderivada de una función a veces es vista con un cierto grado de misticismo a su alrededor. Existen incluso concursos de integración en varias universidades alrededor del mundo, en las cuales el ganador es quien logre encontrar una integral dada con mayor agilidad. Pero, ¿será posible obtener un algoritmo general de integración indefinida, con el cual sea posible integrar cualquier función? De ser así, ¿sería esta una ventaja significativa para quienes conocieran dicho algoritmo de integración?

Más allá de eso, es ampliamente conocido que existen funciones que simplemente no poseen una antiderivada en términos de funciones elementales. Muchas de estas funciones son importantes en aplicaciones de la matemática, y la inexistencia de su antiderivada elemental provoca la necesidad de recurrir a métodos numéricos de integración. Algunos ejemplos de estas funciones son:

- La función e^{-x^2}, que aparece como integrando en la *función error*, la cual es útil en teoría de probabilidades, estadística y ecuaciones diferenciales.
- La función $\frac{\sin(x)}{x}$, que aparece como integrando en la función *seno integral*. Esta y otras integrales de funciones trigonométricas son relevantes en procesamiento de señales.
- La función $\frac{1}{\log(x)}$, que es el integrando en la función *logaritmo integral*. Esta función es importante en la teoría analítica de números, siendo una aproximación asintótica a la función contadora de números primos.
- Las funciones $\frac{1}{\sqrt{(1-x^2)(1-k^2x^2)}}$, que aparecen en el integrando de las *funciones elípticas del primer tipo*. Estas puede utilizarse para expresar la solución de un problema de péndulo simple en física mecánica clásica, sin utilizar aproximaciones de ángulo pequeño.

Ambos problemas descritos sobre la integración indefinida parecen relacionarse al menos ligeramente, pues al buscar un algoritmo de integración simbólica sería evidente la dificultad causada por la imposibilidad de encontrar una antiderivada elemental para ciertas funciones. Esta tesis propone una solución a ambos problemas, a través de un algoritmo de decisión de integrabilidad en términos elementales. Una vez esté demostrado que la antiderivada elemental existe, el mismo algoritmo será capaz de determinar la misma.

El contenido principal de este estudio se encuentra en los capítulos 5 al 10. En el quinto capítulo se presentará una breve introducción a las bases matemáticas más importantes y necesarias para ahondar en el sujeto principal de la tesis. En el sexto capítulo se formaliza a través del álgebra a la derivada e integral como operadores simbólicos. El séptimo capítulo discute de manera formal a las funciones elementales y sus propiedades, hablando en el proceso de la estructura de dichas funciones y la forma que poseen sus derivadas. En el capítulo octavo se busca sentar las bases de un algoritmo más general de integración a través de las funciones racionales, y al mismo tiempo servirá como un ejemplo y vista previa a herramientas que se utilizarán a lo largo del trabajo. El noveno capítulo discute uno de los teoremas fundamentales dentro de la integración simbólica, debido a Liouville. Este teorema exige una forma específica para una función con antiderivada elemental. Se finaliza con el décimo capítulo, que aprovecha los principios de integración discutidos a lo largo del trabajo para crear técnicas de decisión sobre la integrabilidad simbólica de funciones elementales, así como un algoritmo de integración para funciones que sí posean una antiderivada elemental.

En cuanto a su alcance, esta tesis busca encontrar caracterizaciones de las funciones que tengan antiderivadas elementales. Aunque dicha tarea no esté por completo finalizada en la literatura actualmente existente, debido a que usualmente las aproximaciones por métodos numéricos y series infinitas son suficientes para resolver en la práctica el problema de la integración, sí se conocen algunas caracterizaciones de este tipo para ciertos tipos de funciones. Además, en los casos restantes, existen resultados que pueden ayudar a determinar si ciertas antiderivadas son elementales o no. Esto hace de los resultados presentados un semi-algoritmo de decisión. Por otra parte, en este trabajo se demostrará lo necesario para determinar la integrabilidad simbólica de funciones en tres de cuatro tipos de campos de funciones elementales: los campos de *funciones racionales*, los campos cuya última extensión es *logarítmica*, y los campos cuya última extensión es *exponencial*. Aquello que es requerido para campos cuya última extensión es *algebraica* requiere de herramientas de alto calibre en geometría algebraica computacional, por lo cual únicamente se mencionará pero no será demostrado, y se refiere al lector a fuentes más completas en ese aspecto. Una vez expuestas las definiciones y los teoremas, la estructura del semi-algoritmo a desarrollarse será la siguiente.

1. Tomar una función elemental f a integrarse.
2. Identificar el campo de funciones elementales al cual f pertenece, siendo este uno de los cuatro tipos a continuación:
   - Campo de funciones racionales.
   - Campo de extensión logarítmica.
   - Campo de extensión exponencial.
   - Campo de extensión algebraica.
3. Aplicar el algoritmo de reducción de Hermite, de ser necesario.
4. Se decide la integrabilidad simbólica de f a través de los teoremas de Rothstein-Trager y de los teoremas de integración de polinomios logarítmicos/exponenciales/algebraicos.
5. Si f es integrable simbólicamente, los teoremas anteriormente mencionados proveen su solución. De lo contrario, simplemente queda demostrado que la integral es no-elemental.

CAPÍTULO 2

Objetivos

2.1. Objetivo general

Recopilar y ordenar la teoría algebraica diferencial necesaria para construir un procedimiento formal de decisión que permita determinar la existencia o inexistencia de una antiderivada elemental para una función elemental dada.

2.2. Objetivos específicos

- Presentar una *formalización matemática* de la rama del Álgebra Diferencial con una perspectiva enfocada a la Integración Simbólica.
- Definir formalmente el concepto de *función elemental* dentro del álgebra, en busca de caracterizaciones sobre la existencia de una antiderivada en símbolos algebraicos.
- Exponer algoritmos de Integración Simbólica para funciones elementales, partiendo de las *funciones racionales* como pieza clave para trabajar con funciones elementales generales.
- Demostrar teoremas clave que puedan ser utilizados como herramienta para determinar si una función posee, o no, una *antiderivada elemental*.
- Construir un *algoritmo de decisión* sobre integrabilidad simbólica que construya por completo la antiderivada de una función si esta es elemental.

CAPÍTULO 3

Justificación

En el mundo académico adyacente a la matemática, enseñar la mayor cantidad posible de técnicas de integración y resolver cientos de integrales de manera rápida es una práctica común. En esta línea de enseñanza siempre se llega a una pared que detiene, al menos momentáneamente, al educando y al educador: hay integrales indefinidas que parecen no poseer una solución accesible. A veces, simplemente es necesario utilizar maquinaria matemática más fuerte. En otras ocasiones el instinto del estudiante es correcto, y la antiderivada que se busca no puede ser expresada en términos de las funciones que se manejan en un curso introductorio de matemática al nivel de pregrado. ¿Pero cómo podría el estudiante saber esto, si no con una amplia cantidad de trucos matemáticos oscuros, y memorizando exactamente los tipos de integrales que pueden ser resueltas y las que no? En muchas ocasiones, incluso se menciona que ciertas funciones como e^{-x^2} y $\frac{\sin(x)}{x}$, las cuales son aplicadas en la teoría de probabilidades, telecomunicaciones, procesamiento de señales, entre otras ciencias, no poseen una antiderivada elemental. No obstante, la prueba de estos hechos no es ampliamente conocida, y ni siquiera se suele definir con exactitud el significado del término “antiderivada elemental”, creando más misterio alrededor del tema de la integración.

Por la situación descrita, el presente trabajo de investigación se concentra en la profundización y formalización algebraica del concepto de *antiderivada elemental*, y presenta la forma que puede poseer la antiderivada de una función dada dentro del contexto del cálculo integral. También se discuten las condiciones bajo las cuales dicha antiderivada simplemente no puede existir en términos de símbolos conocidos dentro de una variedad de funciones específicas, llamadas *funciones elementales*. El interés en dicho tema también surge debido a la importancia del proceso de integración simbólica dentro de varias ramas de la ciencia y la matemática, y lo misterioso que parece ser el mismo para un estudiante que apenas inicia su aventura en el mundo de la matemática formal.

Se espera que el presente trabajo sirva como referencia para todo aquel instructor que desee dar una respuesta más completa en relación con la pregunta: ¿Por qué hay funciones que “no se pueden integrar”? También se busca que el estudiante curioso pueda responder sus dudas a través de una lectura completa y exhaustiva de este trabajo, creando la capacidad de utilizar los conocimientos adquiridos para cualquier aplicación profesional que decida darle a la integración en la matemática, ciencia e ingeniería. En general, esta tesis intenta hacer más accesibles las demostraciones pertinentes a la inexistencia de antiderivadas elementales, pues se trata de teoremas ampliamente citados, pero difícilmente conocidos incluso por los más estudiosos matemáticos.

CAPÍTULO 4

Antecedentes históricos

El problema de encontrar una función elemental que represente la antiderivada de una función se remonta a tiempos tan tempranos como la creación del cálculo en el siglo XVII. Muchos matemáticos famosos trabajaron años creando técnicas y atajos para encontrar la antiderivada de varios tipos de funciones, pero resultó ser que algunas de estas simplemente parecían ser imposibles de resolver. Como es de esperarse, esto llevó a los matemáticos a la búsqueda de una demostración de inexistencia para estas antiderivadas. Más de un siglo después de los primeros indicios del cálculo, entre los años 1833 y 1841, el matemático francés Joseph Liouville publicó una serie de artículos discutiendo este tema. Entre estos artículos, uno de los más importantes llevó por nombre "*Sur la détermination des intégrales dont la valeur est algébrique*", que en español se traduce como: "*Sobre la evaluación de integrales cuyo valor es algebraico*" [15]. En estos artículos, Liouville logró demostrar por primera vez la inexistencia de algunas antiderivadas en términos de funciones elementales.

A inicios del siglo XX, el famoso G. H. Hardy [9] realizó un compendio sobre integración en una variable. En él, utilizó mucho del trabajo de Liouville para demostrar la inexistencia de varias antiderivadas simbólicas. Más tarde en el siglo XX, el matemático J. F. Ritt [19] formalizó el estudio del Álgebra Diferencial, que sería la herramienta por excelencia para generalizar las demostraciones de Liouville. Más recientemente, Robert H. Risch [18] presentó entre 1968 y 1979 una solución semi-algorítmica al problema de integración simbólica, construyendo su algoritmo de integración y de decisión en cuanto a integrabilidad en términos algebraicos. Este algoritmo fue finalizado con los aportes de Trager [22] y Bronstein [4], quienes presentaron algoritmos de integración de un tipo especial de funciones elementales. En efecto, muchas de las calculadoras de integración simbólica utilizan hoy en día una implementación de los algoritmos propuestos por estos matemáticos.

Aún con este trabajo, existen funciones cuya integrabilidad algebraica es un problema abierto. En el año 2020, D. Masser y U. Zannier [17] encontraron contraejemplos a algunas conjeturas de Davenport [7]. Se han buscado demostraciones e implementaciones alternativas de los teoremas y algoritmos en integración simbólica para su mejoría, pero la literatura y el interés dedicado al tema no son los más extensos. Una de las fuentes más completas, modernas y claras es el libro de *Álgebra Computacional* de K. O. Geddes, S. R. Czapor, y G. Labahn, publicado en 1992 [8]. Este demuestra y resume algunos teoremas y algoritmos que serán discutidos en esta tesis, entre ellos los algoritmos de E. Hermite [11], M. Rothstein [21] y B. Trager [22]; y uno de los teoremas cumbre en integración simbólica, el principio de Liouville.

CAPÍTULO 5

Nociones preliminares

En este capítulo, se presentan definiciones y resultados en algunas áreas de la matemática que serán utilizados a lo largo de la presente investigación. La mayoría de estos resultados no serán demostrados, pues no son más que una base necesaria para entrar al detalle de interés en los siguientes capítulos, y se espera que un estudiante de matemática los conozca o pueda estudiarlos por cuenta propia. Sin embargo, se agrega al inicio de cada sección algunas referencias en las cuales se encuentran las demostraciones correspondientes.

5.1. Álgebra

La información sobre anillos y campos resaltada en esta sección puede ser encontrada en los capítulos 3 y 5 del libro de Herstein [12].

5.1.1. Teoría de anillos

Una de las herramientas principales a utilizarse más adelante son los anillos. Esto se debe a su utilidad a la hora de trabajar con conjuntos de polinomios, los cuales serán herramientas muy importantes en este estudio.

Definición 5.1: Un conjunto no vacío R es un *anillo* si en él se definen dos operaciones binarias con ciertas propiedades. Estas a menudo reciben los nombres de suma $(+)$ y producto $(\cdot)$, usualmente en ese orden. Las propiedades a cumplirse son las que siguen.

1. **Cerradura de la suma:** Si $a \in R$ y $b \in R$, entonces $a + b \in R$.
2. **Asociatividad de la suma:** Para todo $a, b, c \in R$, se cumple $a + (b + c) = (a + b) + c$.
3. **Neutro de la suma:** Existe $0 \in R$ tal que para todo $a \in R$ se cumple $a + 0 = 0 + a = a$.

4. **Inversos de la suma:** Para todo $a \in R$, existe $-a \in R$ tal que $a + (a) = (-a) + a = 0$, donde $0 \in R$ es el neutro aditivo.
5. **Conmutatividad de la suma:** Para todo $a, b \in R$, se tiene $a + b = b + a$.
6. **Cerradura del producto:** Si $a \in R$ y $b \in R$, entonces $a \cdot b \in R$.
7. **Asociatividad del producto:** Para todo $a, b, c \in R$, se cumple $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
8. **Distributividades del producto sobre la suma:** Si $a, b, c \in R$, entonces:

$$c \cdot (a + b) = c \cdot a + c \cdot b,$$
$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

Es decir, $(R, +)$ es un grupo abeliano, mientras $(R - \{0\}, \cdot)$ no necesariamente es conmutativo, no necesariamente posee inversos, y ni siquiera necesita un elemento neutro multiplicativo.

Como se mencionaba, la importancia de los anillos para el propósito de este trabajo radica sobre todo en los anillos de polinomios. Para entender mejor estas estructuras, vale la pena darle un nombre a algunos tipos de anillos que aparecen en su estudio.

Nota Bene 5.1 (Tipos de anillos)**:** Si $(R, +, \cdot)$ es un anillo en el cual todos sus elementos conmutan en multiplicación, entonces R es un *anillo conmutativo*. Por otro lado, si $(R, +, \cdot)$ es un anillo tal que $(R - \{0\}, \cdot)$ forma un grupo, entonces R es un *anillo de división*. Si $(R - \{0\}, \cdot)$ forma un grupo abeliano, entonces R es un *campo*. Ahora, en un anillo R, si $a, b \in R - \{0\}$ cumplen $ab = 0$ entonces se dice que a y b son *divisores de cero*. En caso que R sea un anillo conmutativo y sin divisores de cero, entonces R es un *dominio entero*.

Sean $m \in \mathbb{Z}$ y $a \in R$. Entonces la multiplicación ma significa sumar al elemento $a \in R$ una cantidad de m veces:

$$ma = \underbrace{a + a + \cdots + a}_{m \text{ veces.}}$$

Ahora bien, la *característica* de un dominio entero es el menor entero no negativo que anula a todos sus elementos bajo multiplicación. Un dominio entero D es de *característica 0* si la relación $ma = 0$ para $a \neq 0$ en D y $m \in \mathbb{Z}$ solo puede ocurrir si $m = 0$. Un dominio entero D es de *característica finita* si existe $p \in \mathbb{Z}^+$ tal que $pa = 0$ para todo $a \in D$. En este caso, es fácil demostrar que p es un número primo.

Finalmente, se le llama *anillo euclideano* a aquel dominio entero R que posee una noción de valor absoluto, llamado el d-valor. Este es tal que para todo $a, b \in R - \{0\}$ se tiene que $d(a) \leq d(ab)$, y que existen $q, r \in R$ tales que $a = qb + r$ donde se da una de $r = 0$ o $d(r) < d(b)$. Esto último es un algoritmo de la división abstracto.

Usualmente se trabajará con dominios enteros, pues esta es la forma que los anillos de polinomios toman cuando los coeficientes son parte de un campo. De hecho, estos serán anillos euclideanos, donde el d-valor es el grado de un polinomio.

En los anillos de polinomios, será importante la noción de máximo común divisor. Aunque es un concepto ampliamente conocido, cabe resaltar su definición, la cual requiere conocer la relación de divisibilidad entre elementos.

Definición 5.2: Si R es un anillo conmutativo y $a, b \in R$ con $a \neq 0$. Entonces, se dice que *a divide* a b si existe $c \in R$ tal que $ac = b$. La relación de *divisibilidad* se denota por $a \mid b$.

Con esto, ya es posible definir formalmente al máximo común divisor de dos elementos de un anillo conmutativo dado.

Definición 5.3: Si R es un anillo conmutativo y $a, b \in R$, entonces $d = (a, b) \in R - \{0\}$ es un *máximo común divisor* de a y b en R si se cumplen ambas condiciones siguientes:

- $d \mid a$ y $d \mid b$,
- Si $c \in R - \{0\}$ es tal que $c \mid a$ y $c \mid b$, entonces $c \mid d$.

Es muy importante resaltar que el máximo común divisor en un anillo euclideano es único salvo una clase de equivalencia, la cual se presenta en la relación de asociación de elementos. Para llamar a este concepto, se define qué es una unidad.

Definición 5.4: Sea R un anillo conmutativo con identidad multiplicativa. Un elemento $a \in R$ es una *unidad* si existe $b \in R$ tal que $ab = 1$.

Definición 5.5: Sea R un anillo conmutativo con identidad multiplicativa. Un elemento $a \in R$ es *asociado* a otro elemento $b \in R$ si existe una unidad $u \in R$ tal que $a = ub$.

En efecto, la relación de *ser asociados* es una relación de equivalencia. Muchas propiedades de unicidad se cumplen *salvo asociación*, significando que si un elemento cumple cierta propiedad, sus elementos asociados también la cumplen. El máximo común divisor es único salvo asociación en un anillo euclideano.

El siguiente concepto permite fabricar campos determinados por dominios enteros, construyendo elementos fraccionarios a través de las propiedades comunes de las fracciones. Esta es una forma útil de pensar en ciertos campos con propiedades relacionadas a los cocientes algebraicos.

Definición 5.6: Si D es un dominio entero, el *campo de cocientes* $(F, +, \cdot)$ se construye de tal manera que $a/b = c/d$ si y solo si $ad = bc$, y

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Por ejemplo, si se toma el dominio entero $\mathbb{Z}$ con sus operaciones de suma y producto usuales, su campo de cocientes es $\mathbb{Q}$. Este concepto resulta importante para definir los campos de funciones racionales. Pero primero, se requiere definir los anillos de polinomios.

Definición 5.7: Sea F un campo, entonces se define al *anillo de polinomios*

$$F[x] = \left\{ \sum_{k=0}^{n} a_k x^k : a_k \in F, a_n \neq 0, n \in \mathbb{N} \right\}.$$

Es decir, $F[x]$ es el conjunto de los polinomios en la variable x y coeficientes en F o sobre F. Dado un elemento de $F[x]$, los $a_k \in F$ correspondientes se llaman coeficientes del polinomio. Además, a_n es llamado el coeficiente principal del polinomio.

Estos conjuntos siempre forman un anillo, lo cual requiere una noción de igualdad, de una suma, y de un producto. Además, en esta definición, x es un *símbolo formal.* De esta manera, no es necesario hacer referencia a las propiedades numéricas que podría cumplir, o no, el símbolo x. Esta forma de pensar en los objetos es de alta importancia en el álgebra simbólica, incluyendo el álgebra diferencial que se desarrollará más adelante.

Definición 5.8: Si F es un campo, y se definen $p(x) = \sum_{i=0}^{m} a_i x^i$ y $q(x) = \sum_{j=0}^{n} b_j x^j$ en $F[x]$, entonces se da la *igualdad de polinomios* $p(x) = q(x)$ si y solo si $m = n$ y $a_k = b_k$ para todo k.

Teniendo una forma bien definida de decidir la igualdad de polinomios, únicamente queda definir la suma y producto para afirmar que $F[x]$ es un anillo.

Definición 5.9: Si F es un campo, y se toman $p(x) = \sum_{i=0}^{m} a_i x^i$ y $q(x) = \sum_{j=0}^{n} b_j x^j$ en $F[x]$, entonces se definen las *operaciones de polinomios* con:

$$p(x) + q(x) = \sum_{k=0}^{\text{máx}\{m,n\}} (a_k + b_k)x^k,$$

$$p(x) \cdot q(x) = \sum_{l=0}^{m+n} \left(\sum_{k=0}^{l} a_{l-k} b_k \right) x^l,$$

con $a_i = 0$ cuando $i > m$ y $b_j = 0$ cuando $j > n$.

En efecto, es posible comprobar que $F[x]$ con estas operaciones forma un anillo. De hecho, siendo F un campo, se tiene que $F[x]$ es un anillo con ciertas propiedades especiales.

Nota Bene 5.2 (Sobre la estructura de los anillos de polinomios)**:** Si F es un campo, entonces $(F[x], +, \cdot)$ forma un anillo conmutativo con elemento neutro multiplicativo, donde $+$ y $\cdot$ representan la suma y producto definidos anteriormente. Es más, este será un anillo euclideano, donde el d-valor se define con la función deg presentada más adelante.

Obviamente resulta importante definir el grado de un polinomio, pues varias demostraciones requieren el uso de las propiedades que este trae consigo.

Definición 5.10: Si F es un campo, entonces es posible definir la función $\deg : F[x] - \{0\} \to \mathbb{N}$ tal que si $p(x) = \sum_{i=0}^{m} a_i x^i \in F[x]$, entonces $\deg(p(x)) = m$ es el *grado del polinomio* $p(x)$. Por otro lado, el grado del polinomio 0 no está definido, y si $\deg(q(x)) = 0$, entonces se dice que $q(x) \in F$ es un *polinomio constante*.

A continuación, se escriben algunas propiedades de alta importancia que presenta el grado de los polinomios como función de $F[x]$. Las siguientes demuestran que, en efecto, la función deg es un d-valor en $F[x]$.

Propiedad 5.1: Si F es un campo con $f(x), g(x) \in F[x] - \{0\}$:

- $\deg(fg) = \deg(f) + \deg(g)$.
- $\deg(f) \leq \deg(fg)$.
- *Algoritmo de la división:* Existen polinomios $q(x), r(x) \in F[x]$ tales que se cumple

  $$f(x) = g(x)q(x) + r(x),$$

  donde $r(x) = 0$ o $\deg(r) < \deg(g)$.

Son estas las propiedades que nos permiten afirmar que, para un campo F, entonces $F[x]$ es un anillo euclideano. De esta manera, se adquieren propiedades útiles como la unicidad salvo asociación de máximos comunes divisores.

Otro par de propiedades necesarias en el estudio del álgebra diferencial a trabajarse son las siguientes, análogas al lema de Bézout en la teoría de números.

Propiedad 5.2 (Lemas de Bézout)**:** Si F es un campo con $f(x), g(x) \in F[x] - \{0\}$, entonces:

- *Lema de Bézout:* Si $d(x) = (f(x), g(x)) \in F[x]$ es el máximo común divisor de f y g, entonces existen polinomios $\lambda(x), \mu(x) \in F[x]$ tales que
$$d(x) = \lambda(x)f(x) + \mu(x)g(x).$$
- *Bézout extendido:* Sea $d(x) = (f(x), g(x)) \in F[x]$, y sea $c(x) \in F[x]$ tal que $d(x) \mid c(x)$. Entonces, existen existen polinomios $\lambda(x), \mu(x) \in F[x]$ únicos tales que
$$c(x) = \lambda(x)f(x) + \mu(x)g(x),$$
$$\deg(\lambda(x)) < \deg(g(x)) - \deg(d(x)).$$
Si también se cumple que $\deg(c(x)) < \deg(f(x)) + \deg(g(x)) - \deg(d(x))$, entonces
$$\deg(\mu(x)) < \deg(f(x)) - \deg(d(x)).$$

Esta última extensión del lema de Bézout aparece en el desarrollo de algunos algoritmos que serán de mucho interés. Entre ellos, resalta el algoritmo de Hermite. Otra definición que se utilizará bastante es la de los campos de funciones racionales, que son un caso especial de los campos de adjunción a mencionarse proximamente.

Definición 5.11: Dado un anillo de polinomios $F[x]$, el campo de cocientes de $F[x]$ se denota por $F(x)$. Este es el *campo de las funciones racionales* en la variable x y con coeficientes en F.

Tres tipos esenciales de polinomios en el desarrollo del álgebra diferencial utilizada en este trabajo se presentan a continuación.

Definición 5.12: Si $F[x]$ es un anillo de polinomios con elemento identidad $1 \in F$, entonces un polinomio $p(x) \in F[x]$ es *mónico* si su coeficiente principal es exactamente igual a 1.

Definición 5.13: Si $F[x]$ es un anillo de polinomios con elemento identidad $1 \in F$, entonces un polinomio $p(x) \in F[x]$ es *primitivo* si el máximo común divisor de sus coeficientes es asociado a 1.

Definición 5.14: Si F es un campo, entonces un polinomio no nulo $p(x) \in F[x]$ es *irreducible* en $F[x]$ si siempre que existan $a(x), b(x) \in F[x] - \{0\}$ tales que $p(x) = a(x)b(x)$, se tiene que solo uno de $\deg(a)$ y $\deg(b)$ es 0.

Suele esperarse que haya una única forma de separar un polinomio en factores irreducibles. Esto es cierto cuando los coeficientes pertenecen a un campo, salvo elementos asociados.

Propiedad 5.3: Si F es un campo, entonces todo polinomio en $F[x] - \{0\}$ puede factorizarse de manera única, salvo asociación, como producto de polinomios irreducibles en $F[x]$, o bien, es una unidad del anillo.

Con esto, se poseen todas las bases necesarias en la teoría de anillos para continuar el trabajo con la teoría de campos.

5.1.2. Teoría de campos

A pesar de haberse definido anteriormente entre los distintos tipos de anillos de la nota 5.1, los campos serán tan importantes a la hora de pensar en los conjuntos a los cuales pertenecen las funciones a trabajar que se les otorga su propia definición.

Definición 5.15: Un conjunto no vacío F es un *campo* si en él se definen dos operaciones binarias, a menudo llamadas suma $(+)$ la primera, y producto $(\cdot)$ la segunda, las cuales cumplen con que $(F, +)$ y $(F - \{0\}, \cdot)$ son grupos abelianos, y el producto se distribuye sobre la suma.

Será importante tomar en consideración campos que contienen dentro de ellos a campos más pequeños. A estos campos se les llaman extensiones.

Definición 5.16: Si F y K son campos tales que $F \subseteq K$, se dice que F es *subcampo* de K y que K es una *extensión* o un *campo de extensión* de F.

Más adelante, los campos de extensión serán importantes para definir a ciertos tipos de funciones. En específico, con estos será posible obtener una formalización del concepto de *función elemental.*

Definición 5.17: Si F es un campo y K es una extensión de F, entonces $a \in K$ es *algebraico* sobre F si existe $f(x) \in F[x]$ un polinomio no constante tal que $f(a) = 0$. Es decir, a es una raíz de f.

Uno de los tipos de funciones elementales incluye a las que aparecen en algunas extensiones algebraicas. Su definición será casi completamente paralela a la de los elementos algebraicos. Para comprender qué es exactamente una extensión algebraica y otras extensiones que se le parecen, son necesarios los campos por adjunción.

Definición 5.18: Si F es un campo, K es una extensión de F y $a \in K$, entonces el *campo de adjunción* $F(a)$ es el subcampo más pequeño de K que contiene a F y al elemento a. Además, este equivale al campo de funciones racionales en a sobre F,

$$F(a) = \left\{ \frac{p(a)}{q(a)} : p(x), q(x) \in F[x], q(x) \neq 0 \right\}.$$

A su vez, también puede pensarse en $F(a)$ como el campo de cocientes del anillo $F[a]$, o como la intersección de todos los subcampos de K que contienen a F y al elemento a. En general, si F es un campo, K es una extensión de F y $a_1, \ldots, a_n \in K$, entonces $F(a_1, \ldots, a_n)$ es el subcampo más pequeño de K que contiene a F y a todos los a_k para $1 \leq k \leq n$.

El concepto de campo de adjunción es uno de los más importantes en esta tesis, por lo cual su comprensión es realmente necesaria. Su importancia radica en la formalización de los campos de funciones racionales, pero también en la formalización de otras funciones, en particular las logarítmicas, exponenciales y algebraicas sobre campos de funciones racionales. Esto será útil para definir de manera exacta a las funciones que buscamos llamar elementales. Finalmente, en algunos momentos resultará necesario hablar de los campos de descomposición de ciertos polinomios, los cuales también pueden pensarse como campos de adjunción.

Definición 5.19: Si F es un campo con $f(x) \in F[x]$, una extensión finita E de F es un *campo de descomposición* de $f(x)$ sobre F si $f(x)$ puede factorizarse como el producto de polinomios lineales sobre E, pero en ningún subcampo propio de E.

Estas serán las nociones algebraicas a utilizar en el presente trabajo, y con ellas es posible iniciar a desarrollar algunas otras herramientas necesarias en el mismo.

5.2. Algoritmo de factorización libre de cuadrados

La factorización en factores libres de cuadrados es de alta importancia en el desarrollo de varios algoritmos de integración utilizados en la teoría de integración simbólica, por lo cual se le dedica este espacio. El detalle de la teoría detrás del mismo puede encontrarse en el capítulo 8 del libro de *Álgebra Computacional* de Geddes [8].

Definición 5.20: Sea R un dominio de factorización única, y sea $a(x) \in R[x]$ un polinomio primitivo sobre R. Se dice que $a(x)$ es *libre de cuadrados* si no posee factores repetidos. Es decir, no existe $b(x)$ con $\deg(b) \geq 1$ tal que $b(x)^2 \mid a(x)$. Equivalentemente, un polinomio es libre de cuadrados si no posee raíces múltiples en un campo algebraicamente cerrado que contiene a sus coeficientes. Esto incluye, por ejemplo, a su campo de descomposición.

Será necesario definir la siguiente forma general para escribir cualquier polinomio en sus factores libres de cuadrados.

Definición 5.21: Sea R un dominio de factorización única. La *factorización libre de cuadrados* de un polinomio $p(x) \in R[x]$ es

$$p(x) = \prod_{k=1}^{n} p_k(x)^k,$$

donde cada $p_k(x) \in R[x]$ es libre de cuadrados, y $(p_i(x), p_j(x)) = 1$ siempre que $i \neq j$.

Como punto importante, estas condiciones permiten que algunos de los $p_k(x)$ sean exactamente iguales a 1. Por tanto, $p(x) = (x+3)(x^3-1)^3(x^4-2x)^6$ es una factorización libre de cuadrados con $p_2(x) = p_4(x) = p_5(x) = 1$. Además, algunos de los factores no están factorizados por completo, pues no es necesario que lo estén.

Nota Bene 5.3: Propiedades algebraicas de la derivada.

Más adelante se definirá una noción algebraica del operador diferencial. Por ahora, simplemente será necesario recordar que la derivada actúa sobre funciones (y en específico, sobre polinomios) a través las propiedades a continuación:

$$(f+g)' = f' + g', \qquad (fg)' = f'g + fg', \qquad (f^n)' = nf^{n-1}f'.$$

Estas propiedades son importantes para demostrar los resultados a continuación, y es por ello que ameritan una mención. Más adelante también aparecerán como propiedades dentro del contexto del álgebra diferencial.

Propiedad 5.4 (Caracterización de libertad de cuadrados)**:** Sea F un campo de característica 0, y sea $a(x)$ un polinomio primitivo en $F[x]$. Considérese al máximo común divisor $c(x) = (a(x), a'(x))$. Entonces, $a(x)$ es libre de cuadrados si y solo si $c(x) = 1$.

Esta propiedad permitirá utilizar las propiedades de las derivadas y los máximos comunes divisores para determinar si un polinomio es libre de cuadrados. Esto permite crear el algoritmo de factorización en factores libres de cuadrados, cuya idea se presenta seguidamente.

¿Cuál es la idea del algoritmo? Sea $p(x) = \prod_{k=1}^{n} p_k(x)^k$, donde $p(x)$ está factorizado en sus factores libres de cuadrados. Entonces, diferenciando esta expresión, se obtiene

$$p'(x) = \sum_{k=1}^{n} \left(k p_k(x)^{k-1} p'_k(x) \prod_{j \neq k}^{1 \leq j \leq n} p_j(x)^j \right).$$

Así, se sigue directamente que

$$c(x) = (p(x), p'(x)) = \prod_{k=2}^{n} p_k(x)^{k-1}.$$

Después se define un nuevo polinomio, con

$$w(x) = \frac{p(x)}{c(x)} = \frac{\prod_{k=1}^{n} p_k(x)^k}{\prod_{k=2}^{n} p_k(x)^{k-1}} = p_1(x) \frac{\prod_{k=2}^{n} p_k(x)^k}{\prod_{k=2}^{n} p_k(x)^{k-1}} = \prod_{k=1}^{n} p_k(x).$$

Por otra parte, se define al polinomio $y(x) = (c(x), w(x))$. A través de las expresiones para $c(x)$ y $w(x)$, se tiene

$$y(x) = (c(x), w(x)) = \left(\prod_{k=2}^{n} p_k(x)^{k-1}, \prod_{k=1}^{n} p_k(x) \right) = \prod_{k=2}^{n} p_k(x).$$

Finalmente, esto hace posible encontrar al primer factor $p_1(x)$ a través de

$$p_1(x) = \frac{w(x)}{y(x)}.$$

Con esto, a través del cálculo de los $c(x)$, $w(x)$ y $y(x)$, se obtiene el primer factor libre de cuadrados. Repitiendo este proceso finito de forma exhaustiva para $p_2(x), \ldots, p_n(x)$, se tiene un algoritmo de factorización en factores libres de cuadrados. Este se resume a continuación.

Algoritmo 5.1 (Factorización libre de cuadrados)**:** Aquí, se presenta una receta general que ejecuta la idea del algoritmo de factorización libre de cuadrados. Este algoritmo es de alta importancia en el álgebra computacional, como se podrá apreciar a la hora de enunciar los teoremas de reducción e integración en los capítulos siguientes.

1. Tomar un polinomio primitivo $p(x)$ en con coeficientes en un campo F.
2. Calcular $c(x) = (p(x), p'(x))$, y luego calcular el polinomio $w(x) = p(x)/c(x)$.
3. A partir de aquí, inicializar un contador en $k = 1$ y un polinomio de salida en $P_0(x) = 1$.
4. Calcular $y(x) = (w(x), c(x))$ y luego $z(x) = w(x)/y(x)$.
5. Calcular el siguiente polinomio dada la regla $P_{k+1}(x) = P_k(x) \cdot z(x)^k$.
6. Reemplazar k por $k+1$, reemplazar $w(x)$ por $y(x)$, reemplazar $c(x)$ por $c(x)/y(x)$. Si $c(x) \neq 1$ ir al paso 4. Si $c(x) = 1$ ir al paso 7,
7. El algoritmo termina y se calcula $P_{k+1}(x) = P_k(x) \cdot w(x)^k$, obteniendo el polinomio expresado como su factorización en polinomios libres de cuadrados.

Se ejemplifica el uso de este algoritmo a continuación, con un polinomio significativamente complicado para mostrar varios ciclos del algoritmo. Nótese que también resultaría útil la capacidad de calcular máximos comunes divisores polinomiales de manera algorítmica. Para ello, se refiere al lector al capítulo 7 de Geddes.

Ejemplo 5.1: Factorización libre de cuadrados.

Considérese el polinomio $p(x) = x^7 - 4x^6 - 3x^5 + 12x^4 + 3x^3 - 12x^2 - x + 4$. Entonces su derivada es $p'(x) = 7x^6 - 24x^5 - 15x^4 + 48x^3 + 9x^2 - 24x - 1$. Con esto, $c(x) = (p(x), p'(x)) = x^4 - 2x^2 + 1$, y luego $w(x) = p(x)/c(x) = x^3 - 4x^3 - x + 4$.

- **Ciclo k = 1.** Se tiene $P_1(x) = 1$, $w(x) = p(x)/c(x) = x^3 - 4x^3 - x + 4$, y $c(x) = x^4 - 2x^2 + 1$. Luego, $y(x) = (w(x), c(x)) = x^2 - 1$. Entonces, $z(x) = w(x)/y(x) = x - 4$. Por tanto,

$$P_2(x) = x - 4.$$

- **Ciclo k = 2.** Se tiene $P_2(x) = x - 4$, $w(x) = x^2 - 1$, y $c(x) = \frac{x^4-2x^2+1}{x^2-1} = x^2 - 1$. Luego, $y(x) = (w(x), c(x)) = x^2 - 1$. Además, $z(x) = w(x)/y(x) = 1$. Por tanto,

$$P_3(x) = (x - 4)(1)^2 = x - 4.$$

- **Ciclo k = 3.** Se tiene $P_3(x) = x - 4$, $w(x) = x^2 - 1$, y $c(x) = \frac{x^2-1}{x^2-1} = 1$. Luego, el algoritmo se detiene. Finalmente,

$$P_4(x) = (x - 4)(1)^2(x^2 - 1)^3 = (x - 4)(x^2 - 1)^3.$$

De esta manera, la factorización libre de cuadrados del polinomio es $p(x) = (x - 4)(x^2 - 1)^3$.

Como nota a considerar, hay algoritmos de factorización más eficientes computacionalmente hablando que el que se mostró en esta sección. El libro de Geddes presenta otro algoritmo debido a D. Yun, y también presenta otros algoritmos para factorización libre de cuadrados en campos de característica no nula. Sin embargo, el presentado aquí será suficiente para cumplir los objetivos del presente trabajo.

5.3. Matriz y resultante de Sylvester

El detalle en la teoría detrás de los resultantes de Sylvester puede ahondarse en los capítulos 7 y 9 del libro de *Álgebra Computacional* de Geddes [8].

Definición 5.22: Sean $p(x) = \sum_{k=0}^{m} a_k x^k$ y $q(x) = \sum_{k=0}^{n} b_k x^k$ polinomios no nulos, con coeficientes en un campo F. Entonces, la *matriz de Sylvester* $M(p, q)$ es la matriz de $(m+n) \times (m+n)$ siguiente:

$$M(p,q) = \begin{bmatrix} a_m & a_{m-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & a_0 \\ b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ 0 & b_m & b_{m-1} & \cdots & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & b_0 \end{bmatrix}$$

Nótese que $M(p, q)$ tiene en sus primeras m filas a los coeficientes de $p(x)$ y en sus últimas n filas a los coeficientes de $q(x)$. Esto, empezando desde la izquierda y haciendo un desplazamiento a la derecha en cada fila nueva, llenando los espacios vacíos con ceros.

Definición 5.23: Sean $p(x) = \sum_{k=0}^{m} a_k x^k$ y $q(x) = \sum_{k=0}^{n} b_k x^k$ polinomios no nulos con coeficientes en un campo F. El *resultante de Sylvester* $\text{res}(p, q)$ se define a través de

$$\text{res}(p, q) = \det(M(p, q)),$$

donde det es la función determinante matricial. En caso que al menos uno de los polinomios sea nulo, se define que el resultante es nulo. Si ambos polinomios son constantes no nulas en R, el resultante es exactamente 1. Cuando se desee especificar sobre qué variable se está trabajando para obtener el resultante, se utiliza un subíndice. Por ejemplo, en este caso, podría escribirse también $\text{res}_x(p, q)$.

La utilidad del resultante se presenta inicialmente en el criterio de Sylvester, el cual es una caracterización para los pares de polinomios con un máximo divisor común no constante. Este resultado es corolario del siguiente teorema.

Teorema 5.1 (Sylvester)**:** Sean $p, q \in R[x]$, y supóngase que $m = \deg(p)$ y $n = \deg(q)$ son positivos. Entonces, existen $s, t \in R[x]$ con $\deg(s) < n$ y $\deg(t) < m$ tales que

$$p(x)s(x) + q(x)t(x) = \text{res}(p, q).$$

Escríbase $p(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$ y $q(x) = b_n x^m + b_{n-1}x^{n-1} + \cdots + b_0$. La idea de la prueba de este teorema es multiplicar cada ecuación por un x^k diferente, de forma que se llegue al sistema de $(m + n) \times (m + n)$ a continuación:

$$\begin{bmatrix} a_m & a_{m-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & a_0 \\ b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ 0 & b_m & b_{m-1} & \cdots & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & b_0 \end{bmatrix} \cdot \begin{bmatrix} x^{m+n-1} \\ x^{m+n-2} \\ x^{m+n-3} \\ \vdots \\ \vdots \\ x^2 \\ x \\ 1 \end{bmatrix} = \begin{bmatrix} x^{n-1}p(x) \\ x^{n-2}p(x) \\ \vdots \\ p(x) \\ x^{m-1}q(x) \\ x^{m-2}q(x) \\ \vdots \\ q(x) \end{bmatrix}.$$

Aquí, la matriz es la de Sylvester, $M(p, q)$. El resultado se sigue inmediatamente usando la regla de Cramer para resolver para la última "variable", que en este caso es 1.

Propiedad 5.5 (Criterio de Sylvester)**:** Sean $p, q \in R[x]$, con F un campo. Entonces p y q poseen un factor común no constante si y solo si $\text{res}(p, q) = 0$.

Demostración. Si $\text{res}(p, q) \neq 0$, entonces se tendría que si p y q tienen un divisor común, entonces este divide al resultante. Pero $\text{res}(p, q)$ es constante, por lo cual dicho divisor debe ser constante.

Por el otro lado, si $\text{res}(p, q) = 0$ entonces $p(x)s(x) = -q(x)t(x)$. Supóngase por contradicción que p y q no poseen un factor común no constante. Entonces, $q \mid s$. Pero $\deg(s) < \deg(q)$, por lo cual esto es un absurdo.

■

Propiedades algebraicas del resultante

Algunos resultados computacionales sobre el resultante de Sylvester que nos serán de gran utilidad se presentan a continuación. Estos son los que crearán la relación fundamental entre el álgebra lineal y la integración simbólica dentro de la teoría a desarrollar. La propiedad siguiente permitirá el cálculo fácil de resultantes, mientras que el teorema que le sigue conseguirá encontrar resultantes dada la aparición de un tipo de producto específico.

Propiedad 5.6: Sea R un anillo conmutativo con identidad multiplicativa, sean $f(x) = \sum_{k=0}^{m} a_k x^k$ y $g(x) = \sum_{k=0}^{n} b_k x^k$ en $R[x]$ con $m, n \in \mathbb{Z}^+$, y sea $c \in R$ una constante no nula. Entonces,

- $\operatorname{res}(c, g) = c^n$,
- $\operatorname{res}(f, f) = 0$,
- $\operatorname{res}(f, g) = (-1)^{mn} \operatorname{res}(g, f)$,
- $\operatorname{res}(cf, g) = c^n \operatorname{res}(f, g)$,
- $\operatorname{res}(x^a f, g) = b_0^a \operatorname{res}(f, g)$, siempre que $a \in \mathbb{Z}^+$.

Estos resultados pueden demostrarse a través de la definición del resultante y de las propiedades del determinante.

Teorema 5.2: Sean $f(x) = a_m \prod_{i=1}^{m}(x - \alpha_i)$ y $g(x) = b_n \prod_{i=1}^{n}(x - \beta_i)$ polinomios sobre un dominio entero D. Entonces, se puede expandir el resultante de f y g de las siguientes maneras:

- $\operatorname{res}(f, g) = a_m^n b_n^m \displaystyle\prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j)$,
- $\operatorname{res}(f, g) = a_m^n \displaystyle\prod_{i=1}^{m} g(\alpha_i)$,
- $\operatorname{res}(f, g) = (-1)^{mn} b_n^m \displaystyle\prod_{i=1}^{n} f(\beta_i)$,

La prueba de la primera de estas propiedades usa polinomios simétricos y el criterio de Sylvester para demostrar que todos los posibles $\alpha_i - \beta_j$ dividen a $\operatorname{res}(f, g)$, y usa un corolario de la propiedad anterior: el hecho de que $\operatorname{res}(cp, dq) = c^n d^m \operatorname{res}(p, q)$. El detalle completo de esta demostración puede encontrarse en el libro de Geddes.

Las otras dos propiedades se siguen de la primera. Nótese que:

$$\operatorname{res}(f, g) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) = a_m^n \prod_{i=1}^{m} \left(b_n^m \prod_{j=1}^{n} (\alpha_i - \beta_j) \right) = a_m^n \prod_{i=1}^{m} g(\alpha_i).$$

La tercera propiedad usa la misma técnica, únicamente recordando que $\operatorname{res}(f, g) = (-1)^{mn} \operatorname{res}(g, f)$ gracias al tercer punto de la propiedad 5.6.

Lo que debe concluirse de esta propiedad es que $\operatorname{res}(f, g)$ es un múltiplo constante del producto de f evaluada en todos los ceros de g, o viceversa. Es decir, existe una constante k tal que:

$$\operatorname{res}(f, g) = k \left(\prod_{c \mid g(c)=0} f(c) \right). \tag{5.1}$$

Sea como sea, dado el caso en que $\operatorname{res}(f, g)$ sea un polinomio sobre alguna variable, encontrar los ceros del lado derecho de 5.1 será equivalente a encontrar los ceros del resultante.

5.4. Residuos de una función de variable compleja

En esta sección, se mostrarán principalmente resultados pertinentes a los residuos de una función de una sola variable compleja. Su importancia radica en un argumento que dará la intuición detrás del cumplimiento de uno de los teoremas de Rothstein-Trager. Dichos resultados pueden profundizarse en el capítulo 5 del libro de *Funciones de una Variable Compleja* de J. B. Conway [6].

En el análisis complejo, existen muchas maneras de definir a los residuos de una función de variable compleja. Una de las formas más naturales requiere de la integración de funciones en $\mathbb{C}$ sobre curvas en el plano complejo, mientras otra de ellas hace uso de la representación a través de series de Laurent. Tal vez sea irónico debido a que este trabajo se desenvuelve en el mundo de las integrales, pero en esta ocasión será más fácil abordar el tema a través de las series de Laurent. Debido a que nuestro paseo en el mundo del análisis complejo no es exhaustivo, únicamente se definirán aquellos conceptos que sean sumamente necesarios. Empezamos por el módulo, siendo un concepto ampliamente conocido y una generalización del valor absoluto en $\mathbb{R}$.

Definición 5.24: Sea $z = a + bi \in \mathbb{C}$, donde $a, b \in \mathbb{R}$. Entonces, el *módulo* de z se denota por $|z|$ y define a través del valor

$$|z| = \sqrt{a^2 + b^2}.$$

Este concepto será útil principalmente para definir el dominio de aquellas funciones que podrán poseer un desarrollo en series de Laurent. Para ello aún es necesario un concepto más, el cual es análogo a la diferenciabilidad de funciones reales: la analiticidad.

Definición 5.25: Sea A un subconjunto abierto de $\mathbb{C}$. Se dice que una función $f : A \to \mathbb{C}$ es *analítica* en z_0 si existe su derivada en ese punto, dada por

$$f'(z_0) = \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0} \in \mathbb{C}.$$

Esta definición es completamente análoga a la de diferenciabilidad en $\mathbb{R}$, con la diferencia de que el límite $z \to z_0$ debe tomarse como un límite en $\mathbb{R}^2$.

Ahora, habiendo definido la analiticidad de funciones y una noción de distancia sobre $\mathbb{C}$ a través del módulo, es posible definir la representación de funciones a través de series de Laurent.

Teorema 5.3 (Laurent)**:** Sean $0 \leq R_1 \leq R_2$ y $\beta \in \mathbb{C}$, y defínase a la corona circular dada por $A = \{z \in \mathbb{C} : R_1 < |z - \beta| < R_2\}$. Sea $f : A \to \mathbb{C}$ una función analítica. Entonces, es posible representar a $f(z)$ a través de su *serie de Laurent*:

$$f(z) = \sum_{k=-\infty}^{\infty} c_k (z - \beta)^k.$$

Los coeficientes c_k son llamados coeficientes de Laurent. Esta representación de f es única, y la convergencia de la serie es uniforme y absoluta en el interior de la corona circular A.

Esta definición presenta una nueva manera de representar funciones, y en específico es bastante útil en la representación de funciones racionales, que más adelante buscaremos integrar.

Además de la representación de funciones, las series de Laurent se asocian a puntos importantes de las funciones complejas. En específico, el centro de las coronas circulares sobre las cuales se definen las series de Laurent suelen ser singularidades de la función. Nos interesa un tipo muy especial de singularidad, cuya definición se muestra a continuación.

Definición 5.26: Sea $f : A - \{\beta\} \to \mathbb{C}$ una función analítica, donde A es una región de $\mathbb{C}$ que contiene a $\beta \in \mathbb{C}$. Si existe un número finito de coeficientes de Laurent que son no nulos y tienen índices $k < 0$, se dice que β es un *polo* de f. Si m es el índice negativo con $c_m \neq 0$ tal que $|m|$ sea máximo en el desarrollo de Laurent para f, entonces β es un polo de orden m.

Existen muchos más tipos de singularidades de las funciones en $\mathbb{C}$, pero nuestro interés se concentra únicamente en los polos. A continuación, se muestra un ejemplo de estos conceptos.

Ejemplo 5.2: Considérese a la función que posee un polo en $z = i$, cuyo desarrollo de Laurent alrededor de dicho polo está dado por

$$f(z) = \frac{2}{(z-i)^3} - \frac{2i+4}{z-i} + 4(z-i)^2 + \cdots .$$

Entonces, puede afirmarse que $z = i$ es un polo de orden 3 para f, pues $m = -3$ es el índice negativo con $c_m \neq 0$ tal que $|m| = 3$ sea máximo. En otras palabras, $m = -3$ es el índice más negativo para el cual no se anula su coeficiente de Laurent.

En general, al conocer la representación de Laurent en un polo de una función es posible identificar el orden de ese polo. En cambio, si se conoce el orden de un polo, únicamente se sabe cuál es el índice más negativo para el cual su coeficiente de Laurent no se anula.

Definición 5.27: Sea $f : A \to \mathbb{C}$ una función analítica, donde A es una corona circular definida como en el teorema 5.3. Entonces el coeficiente de Laurent en el índice $k = -1$ es el *residuo* de f con respecto al polo β.

Habiendo definido qué es el residuo de un polo para una función, únicamente hacen falta mecanismos para su cálculo. Estos mecanismos suelen requerir conocer el orden del polo. Por lo tanto, se presenta la siguiente propiedad, la cual es útil para determinar a través de la multiplicidad de los ceros de una función cuál es el orden de los polos correspondientes a su recíproco.

Propiedad 5.7: Sea $f(z)$ una función que posee un cero de multiplicidad m en β. Entonces, la función $g(z) = \frac{1}{f(z)}$ posee un polo de orden m en β.

Finalmente, se presenta un teorema que permite calcular el residuo de un polo en una función a través de un simple límite. La propiedad anterior y este teorema son complementarios, y facilitan el cálculo de residuos sin necesidad de invocar el cálculo de integrales de línea.

Teorema 5.4: Si f posee un polo de orden $m \geq 1$ en $z = \beta$, entonces el residuo γ de f con respecto a β puede encontrarse a través de

$$\gamma = \frac{1}{(m-1)!} \lim_{z \to \beta} \left[\frac{\mathrm{d}^{m-1}}{\mathrm{d}z^{m-1}} (z-\beta)^m f(z) \right].$$

Este teorema será uno de los principales actores en el enlazamiento de los resultantes de Sylvester con la teoría de la integración simbólica, aunque los tres conceptos parezcan aislados entre sí.

Con esto, se han desarrollado la mayoría de nociones necesarias para el desarrollo teórico a presentarse más adelante. Los temas presentados en los siguientes capítulos seguirán una línea más estructurada, en el camino del álgebra diferencial elemental aplicada a la integración simbólica.

CAPÍTULO 6

Operadores diferenciales en un contexto algebraico

Desde el nacimiento del cálculo integral, fue evidente para varios matemáticos del momento que existían funciones cuya antiderivada es imposible de calcular simbólicamente a través de los métodos y algoritmos convencionales de integración. Dada una función $f(x)$, se busca encontrar $g(x)$ tal que $g'(x) = f(x)$, y específicamente se desea expresar esta función como una combinación de operaciones de suma, resta, multiplicación, división y composición entre funciones conocidas (polinomiales, exponenciales, logarítmicas, trigonométricas, entre otras). Estas funciones, salvo algunos matices, reciben el nombre de *funciones elementales*.

El Análisis de Variable Real proporciona un resultado conocido que en primera inspección parece resolver dicho problema, y es que dada una función continua $f : [a, b] \to \mathbb{R}$, esta necesariamente es Riemann-integrable. Por lo tanto una función g tal que $g' = f$ debe existir. Sin embargo, nada en este teorema exige que g tenga las propiedades necesarias para ser una función elemental. El teorema es uno de existencia, mas no expresa ningún tipo de juicio con respecto a la forma de la antiderivada. Es claro, entonces, que la herramienta analítica ampliamente conocida no será la que resuelva el problema.

En la búsqueda de una solución al problema de integración simbólica descrito, resulta necesario convertir el lenguaje analítico en el que se encuentra escrito el cálculo diferencial e integral a un lenguaje algebraico, que es mucho más manejable en cuanto a la manipulación de variables de integración. Para ello, se definen objetos llamados *operadores diferenciales* dentro de anillos o campos, a través de los cuales se buscará una antiderivada. Como se podrá evidenciar más adelante, no siempre será posible encontrar una antiderivada dentro del espacio algebraico en el cual se está trabajando, por lo cual será necesario buscar extensiones algebraicas como se hace en el desarrollo de la Teoría Algebraica de Galois. En contraste a las estrategias conocidas en un curso de pregrado sobre Álgebra de Galois, las extensiones a realizar no serán únicamente numéricas, pues también se extenderán campos con nuevas funciones.

6.1. Anillos y campos diferenciales

Como es de esperarse en el inicio de cualquier teoría matemática, resulta necesario definir el espacio de trabajo. En este caso, la mayoría del tiempo se trabajará sobre campos diferenciales, y por momentos sobre anillos diferenciales. A continuación, se definen dichos espacios y se profundiza en las propiedades de sus objetos.

Definición 6.1: Sea F un anillo o un campo, y sea $D : F \to F$ un mapeo. El mapeo D obtiene el nombre de *derivada* u *operador diferencial* si cumple las siguientes propiedades.

- *Regla de la suma:*
$$D(f+g) = D(f) + D(g). \tag{6.1}$$
- *Regla del producto:*
$$D(fg) = fD(g) + gD(f). \tag{6.2}$$

Notaciones utilizadas ampliamente para un operador diferencial aplicado a una función f con respecto a una variable x incluyen: $f'(x)$, $f_x(x)$, $D_x(f)$, $\frac{\mathrm{d}f}{\mathrm{d}x}$, $\frac{\partial f}{\partial x}$, entre otras. Será necesario mostrar que estos operadores se comportan como la derivada habitual dadas las condiciones correctas.

Definición 6.2: Sea F un anillo o campo de característica 0. Entonces, se dice que F es un *anillo diferencial* o un *campo diferencial* si existe un operador diferencial $D : F \to F$. Este espacio se denota por (F, D).

Con estas dos definiciones, procedemos a mostrar las propiedades esperadas de un operador diferencial dentro de las estructuras algebraicas en las cuales se encontrarán los objetos de interés.

6.1.1. Propiedades del operador diferencial

Siendo (F, D) un espacio diferencial donde F es un campo, las dos reglas definidas sobre el operador diferencial $D : F \to F$ son suficientes para el cumplimiento de las propiedades mostradas a continuación.

Propiedad 6.1 (Derivada del elemento neutro)**:** Siendo $0 \in F$ el neutro aditivo y $1 \in F$ el neutro multiplicativo del campo diferencial F,

$$D(0) = D(1) = 0. \tag{6.3}$$

Demostración. Nótese que

$$D(1) = D(1 \cdot 1) = 1 \cdot D(1) + 1 \cdot D(1) = D(1) + D(1) = 2D(1).$$

Esto implica que $D(1) = 0$. Por otro lado,

$$D(0) = D(0+0) = D(0) + D(0) = 2D(0).$$

De nuevo, esto implica que $D(0) = 0$.

∎

De hecho, si F es un conjunto numérico, esta propiedad puede extenderse a que la derivada de cualquier número racional es necesariamente nula. Esto se demostrará más adelante en la propiedad 6.6, haciendo uso de las propiedades siguientes.

Propiedad 6.2 (Derivada de un inverso aditivo)**:** Dado $f \in F$, entonces

$$D(-f) = -D(f). \tag{6.4}$$

Demostración. Nótese que $0 = D(0) = D(-f + f) = D(-f) + D(f)$. Entonces, $D(-f) = -D(f)$.

■

Con esta propiedad, siempre será posible extraer o insertar un signo negativo en un operador diferencial. Este resultado también es generalizable a la salida de constantes del operador, pero esto se presentará tras definir exactamente qué es una constante en esta teoría.

Propiedad 6.3 (Derivada de un cociente)**:** Dados $f, g \in F$, con $g \neq 0$,

$$D\left(\frac{f}{g}\right) = \frac{gD(f) - fD(g)}{g^2}. \tag{6.5}$$

Demostración. Resulta necesario encontrar primero $D(1/g)$ en términos de g y $D(g)$:

$$0 = D(1) = D\left(g \cdot \frac{1}{g}\right) = gD\left(\frac{1}{g}\right) + \frac{1}{g}D(g) \implies D\left(\frac{1}{g}\right) = -\frac{D(g)}{g^2}.$$

Con esto, no queda mucho por hacer. Se tiene:

$$\begin{aligned} D\left(\frac{f}{g}\right) = D\left(f \cdot \frac{1}{g}\right) &= fD\left(\frac{1}{g}\right) + \frac{1}{g}D(f) \\ &= f\left(-\frac{D(g)}{g^2}\right) + \frac{1}{g}D(f) = \frac{gD(f) - fD(g)}{g^2}. \end{aligned}$$

■

La siguiente propiedad es prácticamente análoga a la regla de la cadena, pero únicamente cuando la función externa es una función potencia entera.

Propiedad 6.4 (Derivada de una potencia)**:** Dado $f \in F$ y $n \in \mathbb{Z}$, con $f \neq 0$,

$$D(f^n) = nf^{n-1}D(f). \tag{6.6}$$

Demostración. Esta prueba se trabajará por casos sobre n. Primero, considérese el caso $n = 0$. Entonces, $D(f^n) = D(f^0) = D(1) = 0 = 0 \cdot f^{-1} \cdot D(f) = nf^{n-1}D(f)$.

Supóngase ahora que $n > 0$. Se procede por inducción. Como caso base, se tiene ya el caso $n = 0$. Tómese entonces la hipótesis inductiva $D(f^{n-1}) = (n-1)f^{n-2}D(f)$, asumiendo así que se cumple el enunciado para $n - 1$. Entonces,

$$\begin{aligned} D(f^n) = D(f \cdot f^{n-1}) &= fD(f^{n-1}) + f^{n-1}D(f) \\ &= f \cdot \left[(n-1)f^{n-2}D(f)\right] + f^{n-1}D(f) \\ &= (n-1)f^{n-1}D(f) + f^{n-1}D(f) = nf^{n-1}D(f). \end{aligned}$$

Finalmente, sea $n < 0$. Entonces $-n > 0$, y se cumple que $D(f^{-n}) = -nf^{-n-1}D(f)$. Luego,

$$0 = D(1) = D(f^n \cdot f^{-n}) = f^n D(f^{-n}) + f^{-n}D(f^n).$$

Por lo tanto, se debe cumplir que $D(f^n) = -f^{2n}D(f^{-n})$. FInalmente, sustituyendo, se obtiene

$$D(f^n) = -f^{2n}D(f^{-n}) = -f^{2n}[-nf^{-n-1}D(f)] = nf^{n-1}D(f).$$

■

Ahora, se presenta una nota que hace alusión a las propiedades diferenciales de los logaritmos. Más adelante, los logaritmos serán construidos en el álgebra diferencial utilizando cocientes similares a los que aparecen aquí.

Nota Bene 6.1: Identidad logarítmica.

Sean $f_1, f_2, \ldots, f_k \in F$, todos distintos de 0, y sean $n_1, n_2, \ldots, n_k \in \mathbb{Z}$. Luego,

$$\frac{D(f_1^{n_1} f_2^{n_2} \cdots f_k^{n_k})}{f_1^{n_1} f_2^{n_2} \cdots f_k^{n_k}} = n_1 \frac{D(f_1)}{f_1} + n_2 \frac{D(f_2)}{f_2} + \cdots + n_k \frac{D(f_k)}{f_k}. \tag{6.7}$$

Demostración. Se procede por inducción sobre k. Como caso base, se toma $k = 1$. Entonces,

$$\frac{D(f_1^{n_1})}{f_1^{n_1}} = \frac{n_1 f^{n_1 - 1} D(f_1)}{f_1^{n_1}} = n_1 \frac{D(f_1)}{f_1}.$$

Ahora, como hipótesis inductiva supóngase que el enunciado se cumple para $k-1$. Es decir,

$$\frac{D(f_1^{n_1} f_2^{n_2} \cdots f_{k-1}^{n_{k-1}})}{f_1^{n_1} f_2^{n_2} \cdots f_{k-1}^{n_{k-1}}} = n_1 \frac{D(f_1)}{f_1} + n_2 \frac{D(f_2)}{f_2} + \cdots + n_{k-1} \frac{D(f_{k-1})}{f_{k-1}}.$$

Desde luego, esto implica que

$$\begin{aligned}
\frac{D(f_1^{n_1} f_2^{n_2} \cdots f_k^{n_k})}{f_1^{n_1} f_2^{n_2} \cdots f_k^{n_k}} &= \frac{D(f_1^{n_1} f_2^{n_2} \cdots f_{k-1}^{n_{k-1}}) f_k^{n_k} + f_1^{n_1} f_2^{n_2} \cdots f_{k-1}^{n_{k-1}} D(f_k^{n_k})}{f_1^{n_1} f_2^{n_2} \cdots f_k^{n_k}} \\
&= \frac{D(f_1^{n_1} f_2^{n_2} \cdots f_{k-1}^{n_{k-1}})}{f_1^{n_1} f_2^{n_2} \cdots f_{k-1}^{n_{k-1}}} + \frac{D(f_k^{n_k})}{f_k^{n_k}} \\
&= n_1 \frac{D(f_1)}{f_1} + n_2 \frac{D(f_2)}{f_2} + \cdots + n_{k-1} \frac{D(f_{k-1})}{f_{k-1}} + n_k \frac{D(f_k)}{f_k}.
\end{aligned}$$

■

Las propiedades aquí demostradas se cumplen para cualquier operador diferencial, sin restricción alguna sobre el campo diferencial. Sin embargo, para los propósitos de la integración simbólica nos interesa un tipo muy especial de anillos y campos diferenciales: los de funciones en una sola variable. A continuación se discutirá la forma que estos dominios poseen.

6.1.2. Dominios de interés

Ahora se busca determinar las condiciones bajo las cuales una función de variable real $f : \mathbb{R} \to \mathbb{R}$ o compleja $f : \mathbb{C} \to \mathbb{C}$ posee una antiderivada elemental. Tendría sentido, entonces, trabajar con un dominio algebraico cuyos escalares pertenezcan al campo $\mathbb{R}$ o $\mathbb{C}$. Por ejemplo, trabajar con el anillo de polinomios $\mathbb{R}[x]$ o con el campo de funciones racionales $\mathbb{C}(x)$, e incluso empezar a agregar nuevos elementos como en $\mathbb{R}(x, e^x)$.

Si se desea resolver el problema de integración simbólica computacionalmente, se encuentra una desventaja en la utilización de los conjuntos numéricos $\mathbb{R}$ y $\mathbb{C}$, debido a la presencia de números irracionales y trascendentales. Por lo tanto, en cuanto a la implementación en sistemas de álgebra computacional, es más sencillo trabajar usando como base al campo $\mathbb{Q}$. De requerir otros números, reales o complejos, simplemente se requeriría de adjuntar los números necesarios, ya sean algebraicos o trascendentales. Aún así, para los propósitos de esta investigación, este no es un gran problema, pues la implementación de los algoritmos a discutirse no es la meta final.

Justificado esto, se trabajará exclusivamente con subcampos de $\mathbb{C}$, y se utilizarán frecuentemente adjunciones de funciones a estos campo. Entonces, será necesario hablar de extensiones de campos diferenciales. Al extender estos campos, también será necesario asegurarse que los operadores diferenciales coincidan. Por ello, se definen los campos de extensión diferenciales como se observa a continuación.

Definición 6.3: Sean F y G campos diferenciales, con operadores diferenciales D_F y D_G. Se dice que G es un *campo de extensión diferencial* de F si G es una extensión de F y si $D_F(f) = D_G(f)$ para todo $f \in F$.

También en la vía de acercarse a lo conocido en el cálculo, es necesario definir qué es exactamente una constante en esta teoría. Esto se logra a través de los campos de constantes.

Definición 6.4: Sea F un campo diferencial con operador diferencial D. Entonces, el *campo de constantes* de F se define como $\text{con}(F) = \{c \in F : D(c) = 0\}$.

Como su nombre lo indica, este conjunto posee una estructura de campo, lo cual se verifica a continuación demostrando que es subcampo de F.

Demostración. Escríbase $K = \text{con}(F)$. Claramente, $K \subseteq F$. Para demostrar que K es subcampo, únicamente es necesario demostrar que es no vacío, y que para todo $x, y \in K$ con $y \neq 0$ se tiene $x - y \in K$ y $x/y \in K$. Como $D(1) = 0$, es claro que $1 \in K$, de manera que $K \neq \emptyset$. Además $D(x) = D(y) = 0$, lo cual inmediatamente hace $D(x-y) = 0$, de manera que $x-y \in K$. Finalmente,

$$D\left(\frac{x}{y}\right) = \frac{yD(x) - xD(y)}{y^2} = \frac{0}{y^2} = 0.$$

Así, se tiene $x/y \in K$. Con esto, K es un campo.

■

Propiedad 6.5: Sea K un subcampo de $\mathbb{C}$. Entonces, el campo $K(x)$ dotado de un operador diferencial $D : K(x) \to K(x)$ para el cual se toma $D(x) = 1$ es un campo diferencial.

Este campo diferencial posee varias propiedades que requieren una mención, dada su importancia a la hora de ampliar la teoría de integración simbólica. Empezamos por encontrar sus constantes.

Propiedad 6.6 (Diferenciación de números en $\mathbb{Q}$)**:** En un campo diferencial F que contiene a $\mathbb{Q}$, se cumple $D(c) = 0$ para todo $c \in \mathbb{Q}$.

Demostración. La prueba procede por casos sobre los subconjuntos numéricos de $\mathbb{Q}$. Considérese primero $c \in \mathbb{N} \subseteq \mathbb{Q}$. Por la linealidad de D, se tiene

$$D(c) = D(c - 1 + 1) = D(c - 1) + D(1) = D(c - 1).$$

Se puede realizar lo mismo para $c-1$ y llegar a $D(c-1) = D(c-2)$. Siguiendo el proceso de manera inductiva, se llega a que $D(c) = D(c - 1) = \cdots = D(1) = 0$. Ahora, dado que $D(-c) = -D(c)$, entonces $D(-c) = 0$ también, cumpliendo el resultado para todo $c \in \mathbb{Z} \subseteq \mathbb{Q}$. Para finalizar, sea $c = m/n \in \mathbb{Q}$. Es claro que $D(m) = D(n) = 0$ por lo anterior, y usando la derivada de un cociente,

$$D(c) = D\left(\frac{m}{n}\right) = \frac{nD(m) - mD(n)}{n^2} = \frac{0}{n^2} = 0.$$

■

Con esto, el operador diferencial mapea cualquier número racional al 0. Esto nos invita a preguntarnos: ¿Es esto necesariamente cierto para cualquier número real o complejo?

Nota Bene 6.2: Constantes en $\mathbb{R}$ y $\mathbb{C}$.

Para $c \in \mathbb{R}$ y $c \in \mathbb{C}$, no es posible demostrar que $D(c) = 0$. Uno podría pensar en crear una sucesión (c_n) de números racionales convergente a un número real c, y hacer

$$D(c) = D\left(\lim_{n\to\infty} c_n\right) = \lim_{n\to\infty} D(c_n) = 0.$$

Sin embargo, el análisis funcional demuestra que el operador diferencial usual no es continuo, por lo cual no es posible intercambiar el límite dentro de él.

De hecho, realmente solo es cierto que si para $\alpha \in \mathbb{C}$ existe un polinomio $p(x) \in \mathbb{Q}[x]$ tal que $p(\alpha) = 0$, entonces $D(\alpha) = 0$. Esto, debido a que si $p(x) = \sum_{k=0}^{n} a_k x^k$, entonces

$$0 = D(0) = D(p(\alpha)) = D\left(\sum_{k=0}^{n} a_k\alpha^k\right) = D(\alpha)\cdot\left[\sum_{k=0}^{n-1}(k+1)a_{k+1}\alpha^k\right].$$

Asumiendo que $p(x)$ es el polinomio mínimo que anula a α, entonces $\sum_{k=0}^{n-1}(k+1)a_{k+1}\alpha^k \neq 0$, de lo cual $D(\alpha) = 0$. Con esto, todo número algebraico es anulado por D. Así, obtenemos resultados deseables como que $D(\sqrt{2}) = 0$, y lo mismo es cierto para cualquier radical. Pero para números no algebraicos como π o e no hay tanta suerte.

Si $c \in \mathbb{C}$ no es algebraico, entonces es llamado trascendental. Resulta que cualquier número trascendental es tan algebraicamente independiente de los números algebraicos como lo es el símbolo x. De esta manera, es posible elegir cualquier valor que se desee dentro del campo diferencial para $D(\pi)$ o $D(e)$, por ejemplo. Para que el operador diferencial actúe exactamente como en el cálculo, simplemente se definirá en todo momento que la derivada de cada elemento en un conjunto numérico es 0, como usualmente puede demostrarse con la definición analítica de la derivada. Así, tomando $D(x) = 1$, entonces $\mathrm{con}(K(x)) = K$ para cualquier subcampo K de $\mathbb{C}$.

Habiendo aclarado el comportamiento de las constantes en el álgebra diferencial, podemos empezar a extraer resultados deseables como los que se presentan a continuación.

Propiedad 6.7 (Salida de constantes del operador)**:** En el campo diferencial $K(x)$ con $D(x) = 1$, si $q \in \mathrm{con}(K(x))$ y $f \in K(x)$, entonces $D(qf) = qD(f)$.

Demostración. Considérese $D(qf)$. Como $q \in \mathrm{con}(K(x))$, entonces $D(q) = 0$, y se tiene

$$D(qf) = qD(f) + fD(q) = qD(f).$$

∎

Juntando las propiedades anteriormente demostradas, es posible encontrar una forma general de diferenciar polinomios. Esto se presenta en la siguiente propiedad.

Propiedad 6.8 (Diferenciación de polinomios)**:** Sea K subcampo de $\mathbb{C}$. En el anillo diferencial $K[x] \subseteq K(x)$ con $D(x) = 1$, si $p(x) \in K[x]$, entonces $D(p) \in K[x]$. Es decir, el anillo diferencial $K[x]$ es cerrado bajo el operador diferencial D.

Demostración. Sea $n = \deg(p)$. Primero, supóngase que $n = 0$. Entonces $p \in K$, y por la propiedad 6.6 y la discusión que le sigue en la Nota Bene 6.2 se tiene $D(p) = 0 \in K[x]$.

Tomemos, ahora, que $n > 0$. Sea $p(x) = \sum_{k=0}^{n} a_k x^k$ con $a_k \in K$. Entonces, aplicando las propiedades 6.6 y 6.7, se tiene

$$D(p) = D\left(\sum_{k=0}^{n} a_k x^k\right) = D\left(a_0 + \sum_{k=1}^{n} a_k x^k\right) = D(a_0) + \sum_{k=1}^{n} D(a_k x^k) = \sum_{k=1}^{n} a_k D(x^k).$$

Ahora bien, usando la propiedad 6.4, $D(x^k) = kx^{k-1}D(x) = kx^{k-1}$. De esta manera, se llega a que

$$D(p) = \sum_{k=1}^{n} k a_k x^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} x^k \in K[x].$$

■

Como corolario directo de este resultado, se obtiene también que si el grado de un polinomio es $n > 0$, entonces el grado de su derivada es $n - 1$. Además, se obtiene también la forma exacta de dicha derivada, la cual de nuevo es la esperada según lo conocido del cálculo. Asimismo, es claro ahora que D es exactamente el operador diferencial usual del análisis en $K(x)$, pues al usar la regla del cociente en el resultado obtenido se obtendría la derivada esperada de una función racional. Con estas propiedades, el álgebra es suficiente para iniciar a explorar el concepto de la antidiferenciación fuera de la vía del Análisis de Variable Real.

6.2. El problema de la integración simbólica

Como se mencionó con anterioridad, el problema de integración simbólica es bastante simple. Se posee una función f, y se desea encontrar una función g tal que $f = g'$. En la notación establecida, esto se escribiría como $f = D(g)$. Escrito de otra manera, y bajo un pequeño abuso de notación, encontrar g se reduciría a notar que $g = D^{-1}(f)$. Por lo regular, para una función antidiferenciable existen infinitas antiderivadas, pero todas difieren por una constante arbitraria. Tomando esto en cuenta, ¿bajo qué condiciones tiene sentido hablar de D^{-1}?

6.2.1. Antiderivadas y sus propiedades

Para encontrar las problemáticas que pueden haber en la antidiferenciación algebraica, se define primero lo que es una antiderivada.

Definición 6.5: Sea F un campo diferencial con operador $D : F \to F$, y sea G un campo diferencial de extensión de F. El operador $\int : F \to G$ es tal que $D_G \circ \int$ es el operador identidad. Esto es, para $f \in F$, entonces $D_G(\int f) = f$. Al operador $\int$ se le llama *operador antiderivada*, y $\int f$ es una antiderivada de f.

Se define el operador de esta manera dado que, en cálculo, se tendría que $\int \circ D$ es la función original salvo la adición de una constante. Para omitir este problema se ignorarán las constantes de integración, lo cual se justifica seguidamente.

Propiedad 6.9: Sean $f, g \in F$ tales que $D(f) = D(g)$. Entonces, f y g difieren por una constante.

Demostración. Supóngase que $D(f) = D(g)$. Pero entonces, $D(f - g) = D(f) - D(g) = 0$. Esto implica que $f - g \in \mathrm{con}(F)$. Es decir, $f - g = C$ para $C \in \mathrm{con}(F)$, y entonces $f = g + C$.

■

Nota Bene 6.3: Clase de equivalencia de diferencia por una constante.

A menos que se establezca lo contrario, se tomará igualdad de funciones en base a la clase de equivalencia de las funciones que difieren por una constante. Por lo tanto, la propiedad 6.9 realmente significa que si $D(f) = D(g)$ entonces $f \equiv g$ bajo la clase de equivalencia. Además, tomando esta clase de equivalencia, los operadores derivada y antiderivada se cancelan por completo. Esto se observa en la propiedad a continuación.

Propiedad 6.10: Sea F un campo diferencial con $f \in F$, y sea G una extensión de F para la cual $\int f \in G$. Dados $a, b \in G$, escríbase $a \equiv b$ cuando se da $a = b + C$, para $C \in \mathrm{con}(G)$. Entonces

$$\int D(f) \equiv f.$$

Demostración. Sea $f \in F$, y sea G la extensión diferencial de F relacionado a la antiderivada de f. Considérese $\int D(f) \in G$. Entonces,

$$D_G\left(\int D(f)\right) = D(f) = D_G(f).$$

Por la propiedad 6.9, esto implica que $\int D(f) = f + C$ para algún $C \in \mathrm{con}(G)$. Luego, se obtiene lo deseado en la clase de equivalencia: $\int D(f) \equiv f$.

■

De esta manera, al trabajar dentro de las clases de equivalencia de igualdad salvo diferencia por una constante, se tiene que $D \circ \int = \int \circ D = I$, donde I es el operador identidad. Esta propiedad permite pensar en la derivada y la antiderivada como opuestos, sin importar el orden.

Antes de presentar los problemas de antidiferenciación en el álgebra diferencial, mostramos algunas propiedades útiles del operador antiderivada.

Propiedad 6.11 (Homogeneidad de la antiderivada)**:** Sea $f \in F$ y $k \in \mathrm{con}(F)$. Luego,

$$\int kf = k \int f.$$

Demostración. Por la definición de antiderivada, $D\left(\int f\right) = f$ y también $D\left(\int kf\right) = kf$. Juntando esto con la propiedad 6.7 de salida de constantes de la derivada,

$$D\left(k \int f\right) = kD\left(\int f\right) = kf = D\left(\int kf\right).$$

Finalmente, cancelando el operador diferencial, $k \int f = \int kf$.

■

De esta manera, es posible introducir y sacar a gusto las constantes que se multipliquen dentro o fuera de una antiderivada.

Propiedad 6.12 (Aditividad de la antiderivada)**:** Sean $f, g \in F$. Entonces, $\int(f+g) = \int f + \int g$.

Demostración. Nótese que $D\left(\int(f+g)\right) = f + g$ por definición de antiderivada. Por otro lado, similarmente, se tiene por regla de la suma

$$D\left(\int f + \int g\right) = D\left(\int f\right) + D\left(\int g\right) = f + g.$$

Por lo tanto, $D\left(\int(f+g)\right) = D\left(\int f + \int g\right)$. Al cancelar el operador diferencial, se obtiene el resultado deseado. En conjunto con la propiedad 6.11, esto muestra que $\int$ es un operador lineal.

$\blacksquare$

Propiedad 6.13 (Integración por partes)**:** Sea F un campo diferencial con $u, v \in F$. Luego,

$$\int uD(v) = uv - \int vD(u).$$

Demostración. Nótese que $D\left(\int vD(u)\right) = vD(u)$. Por lo tanto,

$$D\left(uv - \int vD(u)\right) = D(uv) - vD(u) = [uD(v) + vD(u)] - vD(u) = uD(v).$$

Aplicando $\int$ de ambos lados, es claro que $\int uD(v) = uv - \int vD(u)$.

$\blacksquare$

La integración por partes es la manera de establecer un procedimiento inverso a la regla del producto. Esta será muy útil en uno de los algoritmos que se presentarán en los siguientes capítulos. Por ahora, movemos la discusión a los problemas que se presentan a la hora de buscar una antiderivada simbólica.

6.2.2. Problemas en la cerradura de la antidiferenciación

Antes de pensar en dominios para los cuales en ocasiones resulte difícil encontrar antiderivadas, presentamos el primer "algoritmo" de antidiferenciación: una manera sistemática de encontrar la antiderivada de cualquier polinomio.

Propiedad 6.14 (Antidiferenciación de polinomios)**:** Sea K un campo. Si $p(x) \in K[x]$, entonces existe $q(x) \in K[x]$ tal que $q(x) = \int p$.

Demostración. Sea $p = \sum_{k=0}^{n} a_k x^k$, y considérese al polinomio $q = \sum_{k=0}^{n} \frac{a_k}{k+1} x^{k+1}$. Es claro que $p = D(q)$, con lo cual $q = \int p$.

$\blacksquare$

Se tiene, de esta manera, un dominio bajo el cual el operador $\int$ es cerrado. No solo eso: también se encontró la forma simbólica de la antiderivada de cualquier polinomio. Sin embargo, resulta que es posible encontrar casos en los cuales $\int$ necesita salirse del dominio original de trabajo. Tal vez el ejemplo más inmediato es recordar que la antiderivada de $1/x$ requiere de la existencia de un *logaritmo*, el cual claramente no es parte del campo $K(x)$. A continuación se demuestra este hecho.

Teorema 6.1: Dado un campo diferencial F con operador diferencial $D : F \to F$, pueden existir funciones $f \in F$ tales que $\int f \notin F$.

Demostración. Se procede con el contraejemplo de $f(x) = 1/x$. Supóngase que $\int 1/x \in K(x)$, con lo cual existe una función $p/q \in K(x)$ tal que $D(p/q) = 1/x$ y $(p, q) = 1$, con $p, q \in K[x]$. Entonces,

$$\frac{qD(p) - pD(q)}{q^2} = \frac{1}{x} \implies xqD(p) - xpD(q) = q^2.$$

Como es claro que $qD(p) - pD(q)$ no puede ser 0 (o se tendría que $1/x = 0$), entonces se tiene que $x \mid q^2$, y por lo tanto $x \mid q$. Luego, es posible escribir $q = x^n t$ para $n \geq 1$, $t \in K[x]$, y $(t, x) = 1$. Reemplazando q por esta expresión, se obtiene

$$x^{n+1}tD(p) - xpD(x^n t) = x^{2n}t^2.$$

Expandiendo la expresión $D(x^n t)$, esta ecuación equivale a

$$x^{n+1}tD(p) - nx^n pt - x^{n+1}pD(t) = x^{2n}t^2.$$

Y tras algunas manipulaciones algebraicas sencillas,

$$npt = x[tD(p) - pD(t) - x^{n-1}t^2].$$

Esto es, $x \mid pt$. Pero $(t, x) = 1$, por lo cual $x \mid p$. De esta manera se llega a que p y q presentan un factor común en x, cuando $(p, q) = 1$. Habiendo llegado a un absurdo, se concluye que $\int 1/x \notin K(x)$.

■

Resulta necesario definir una nueva clase de funciones para encontrar antiderivadas de funciones como esta. En este caso, al hablar de la antiderivada de la función $1/x$, en el capítulo siguiente se procederá a definir algebraicamente al logaritmo. Esto resolverá el problema de antidiferenciación propuesto por completo. ¿Pero a qué nos referimos con *resolver un problema de antidiferenciación*? La siguiente nota busca aclarar esta cuestión.

Nota Bene 6.4: Proceso de integración entre campos diferenciales.

Sea F un campo diferencial, y considérese una función $f \in F$ para la cual se desea encontrar simbólicamente $\int f$. Como se discutió previamente, este objeto no necesariamente se encontrará en F. Por lo tanto, el proceso de integración entre campos diferenciales se empeñará en encontrar una extensión G de F de la forma $G = F(g_1, g_2, \ldots, g_n)$ en la cual exista $g \in G$ tal que $g = \int f$. O bien, en ciertos casos, demostrar que una extensión de este tipo no puede existir.

En el caso de $K(x)$, se afirma que las extensiones necesarias para encontrar todas las antiderivadas únicamente requieren de nuevas constantes y logaritmos, como podrían ser $\sqrt{2}$ y $\log(x + i)$. El capítulo 8 se concentrará en demostrar esta afirmación, y por el momento nos cuestionaremos si esto realmente tiene sentido según lo que se conoce del cálculo.

Existe una gran cantidad de funciones para las cuales se desea conocer su integrabilidad, pero resulta que el problema general de integración simbólica puede ser resuelto pensando únicamente en tres tipos de extensiones de campo diferencial, a definirse en el siguiente capítulo: logarítmicas, exponenciales, y algebraicas. En buena parte, esto es gracias a la flexibilidad de las funciones elementales al considerarlas como funciones en $\mathbb{C}$. Por ejemplo, es posible notar que todas las funciones trigonométricas y sus inversos son en realidad combinaciones de funciones algebraicas, exponenciales y logarítmicas en $\mathbb{C}$. Esto se muestra más a detalle en el Anexo 14.1, y también se observa cómo juega en algunos ejemplos al final de este capítulo.

Cabe mencionar que, si no se desea hacer el viaje a los números complejos, también es posible resolver completamente el problema únicamente en $\mathbb{R}$. Esto requiere de dos tipos más de funciones: tangentes y tangentes inversos. Si se desea ahondar en esto, puede consultarse los artículos de Risch [18] y de Bronstein [4]. En este trabajo, todo se realizará haciendo un pequeño paso a través del mundo de los números complejos cuando sea necesario.

A partir de este punto, el operador antiderivada $\int f$ tomará la notación habitual $\int f(x)\,\mathrm{d}x$ cuando el contexto lo amerite, y se ignorarán las constantes de integración a menos que se especifique lo contrario. Las extensiones se escribirán como $K(x, f_1, f_2, \ldots, f_n)$, donde K es un subcampo de $\mathbb{C}$, y donde los f_i serán las funciones añadidas al campo diferencial. Además, se supondrá siempre que todo elemento de K es constante, y que $D(x) = 1$. Finalmente, se utilizará el término *Integral* para referirnos a la antiderivada de una función, haciendo alusión a la integral indefinida.

El ejemplo siguiente muestra un caso en el cual, aunque suene contradictorio a la experiencia, la antiderivada de una función racional está dada por logaritmos.

Ejemplo 6.1: Considérese la siguiente antiderivada, comúnmente encontrada en un curso introductorio de cálculo Integral de pregrado:

$$\int \frac{1}{1+x^2}\,\mathrm{d}x = \tan^{-1}(x).$$

En primera inspección, el integrando se encuentra en el campo diferencial $\mathbb{Q}(x)$, pero la antiderivada no parece encontrarse en una extensión logarítmica del mismo. Sin embargo, nótese que

$$\int \frac{1}{1+x^2}\,\mathrm{d}x = \int \frac{1}{(x-i)(x+i)}\,\mathrm{d}x = \frac{1}{2i}\int \left(\frac{1}{x-i} - \frac{1}{x+i}\right)\mathrm{d}x = \frac{1}{2i}\log(x-i) - \frac{1}{2i}\log(x+i).$$

Se ignora por el momento el procedimiento de solución de la integral, pues dicho tema se esclarecerá más adelante. Enfocándose en el resultado, se observa que en este caso el campo diferencial de extensión necesario para encontrar una antiderivada es $\mathbb{Q}(x, i, \log(x+i), \log(x-i))$. Esto concuerda con la afirmación, y como se verá más adelante, es posible demostrar la veracidad de la misma.

Terminamos este capítulo con otro ejemplo de una integral que motiva a pensar en algoritmos de integración de funciones racionales.

Ejemplo 6.2: Considérese la integral $\int \frac{1}{x^2-k}\,\mathrm{d}x$. Se puede observar que

$$\begin{aligned}\int \frac{1}{x^2-k}\,\mathrm{d}x = \int \frac{1}{(x-\sqrt{k})(x+\sqrt{k})}\,\mathrm{d}x &= \frac{1}{2\sqrt{k}}\int \left(\frac{1}{x-\sqrt{k}} - \frac{1}{x+\sqrt{k}}\right)\mathrm{d}x \\ &= \frac{1}{2\sqrt{k}}\log\left(x-\sqrt{k}\right) - \frac{1}{2\sqrt{k}}\log\left(x+\sqrt{k}\right).\end{aligned}$$

Aquí, la antiderivada pertenece a $\mathbb{Q}(\sqrt{k})\left(x, \log\left(x-\sqrt{k}\right), \log\left(x+\sqrt{k}\right)\right)$, mientras que la función original pertenece a $\mathbb{Q}(x)$.

Otra forma de llegar a esta respuesta es a través de la sustitución trigonométrica. Se puede tomar $x = \sqrt{k}\sec(\theta)$, y entonces $\mathrm{d}x = \sqrt{k}\sec(\theta)\tan(\theta)\,\mathrm{d}\theta$. Además, $x^2 - k = k(\sec^2(\theta) - 1) = k\tan^2(\theta)$. Con esto,

$$\int \frac{1}{x^2-k}\,\mathrm{d}x = \int \frac{1}{k\tan^2(\theta)}\sqrt{k}\sec(\theta)\tan(\theta)\,\mathrm{d}\theta = \frac{1}{\sqrt{k}}\int \csc(\theta)\,\mathrm{d}\theta\,.$$

La integral del cosecante está dada por $-\log(\csc(\theta) + \cot(\theta))$. Es posible expresar $\csc(\theta)$ y $\cot(\theta)$ en términos de x, con lo cual

$$\frac{1}{\sqrt{k}}\int \csc(\theta)\,\mathrm{d}\theta = -\frac{1}{\sqrt{k}}\log(\csc(\theta) + \cot(\theta)) = -\frac{1}{\sqrt{k}}\log\left(\frac{\sqrt{x+\sqrt{k}}}{\sqrt{x-\sqrt{k}}}\right).$$

Y por las propiedades del logaritmo en el cálculo, esta antiderivada es equivalente a la encontrada usando fracciones parciales.

En este ejemplo, como en el anterior, que es el caso especial $k = -1$, se procedió con técnicas de integración básicas como en un curso introductorio al cálculo integral. Sin embargo, para funciones racionales más complejas, es importante pensar en algoritmos que tomen una función y obtengan su antiderivada después de una serie finita de pasos de fácil replicación. En el siguiente capítulo, se ahondará en algunos algoritmos de integración simbólica que permitirán manipular algebraicamente al integrando y a la integral para separarla en piezas, o bien, resolverla por completo.

CAPÍTULO 7

Funciones elementales y su estructura

Uno de los principales objetivos del presente trabajo es, dada una función, lograr deducir correctamente si esta posee una antiderivada expresable en términos de funciones conocidas. ¿Pero a qué funciones se les da el privilegio de ser llamadas "conocidas"? Es necesario encontrar una definición simple y alineada a la intuición de lo que una función de este tipo podría ser, y esta es una de las tareas de este capítulo. Básicamente, se buscará que las funciones a trabajar sean todas aquellas que puedan aparecer dentro de una integral definida en un curso de cálculo.

Como se ha discutido con anterioridad, a dichas funciones se les llama *Funciones Elementales*. Estas están formadas por una cantidad finita de sumas, diferencias, productos, cocientes y composiciones de funciones polinómicas, radicales, racionales, exponenciales, logarítmicas, trigonométricas y sus inversas, hiperbólicas y sus inversas, entre otras. Sin embargo, esta es una forma muy complicada de describir lo que buscamos que una función elemental sea. Se utilizará una forma aún más simple de definirlas, y se discutirá sobre la estructura que posee un campo de estas funciones.

7.1. El teorema estructural de las funciones elementales

La forma en que se definirán las funciones elementales provoca que las mismas posean una estructura bastante particular. Esto resulta en un teorema estructural, el cual es bastante importante en el Álgebra Diferencial, y requiere de bastante maquinaria algebraica que fue desarrollada por Ritt [19] y Risch [18], entre otros. Dicho teorema tiene fuertes implicaciones que se discutirán más adelante, y es por ello que mencionarlo es tan valioso. Sin embargo, dado que se sale del alcance de este trabajo de investigación, el teorema no será demostrado.

Antes de entrar de lleno a la estructura de las funciones elementales, empezamos por definir algunos conceptos del análisis en términos algebraicos, y por demostrar algunas propiedades conocidas en el contexto del álgebra.

7.1.1. Tipos de funciones elementales

Como se discutió en el capítulo 6, resulta necesario definir a las funciones logarítmicas para poder integrar simbólicamente a ciertas funciones racionales. Por su importancia en el desarrollo de este trabajo, es el primer nuevo tipo de función elemental a definirse.

Definición 7.1: Sea F un campo diferencial, y sea G una extensión diferencial de F. Sea $g \in G$ tal que existe $f \in F$ que cumple la ecuación diferencial

$$D(g) = \frac{D(f)}{f}.$$

Entonces, se dice que g es un *logaritmo* sobre F, o que es *logarítmica* sobre F. Esto se denota a través de $g = \log(f)$.

Con esta definición, el problema que surge al antidiferenciar $1/x$ tiene solución. Es posible encontrar la función $g = \log(x)$, la cual cumple

$$D(g) = \frac{D(x)}{x} = \frac{1}{x}.$$

Así, se argumenta que aunque la antiderivada de $1/x$ no yace en $F = K(x)$, puede encontrarse en una simple extensión del campo: $G = K(x, \log(x))$. Luego, si se toma a los logaritmos como una de las funciones fundamentales a trabajar, entonces la antiderivada de $1/x$ no presenta ningún problema. Además, es posible comprobar que el logaritmo algebraico definido cumple con las propiedades esperadas de los logaritmos. Se presentan aquí las dos más importantes.

Propiedad 7.1: Sea F un campo diferencial, y sean $f, g \in F$. Entonces,

$$\log(fg) = \log(f) + \log(g). \tag{7.1}$$

Demostración. Considérese $\theta = \log(fg)$. Luego, por definición 7.1 y por la regla del producto,

$$D(\theta) = \frac{D(fg)}{fg} = \frac{gD(f) + fD(g)}{fg} = \frac{D(f)}{f} + \frac{D(g)}{g} = D(\log(f) + \log(g)).$$

Cancelando el operador diferencial, $\log(fg) = \log(f) + \log(g)$.

■

Esta propiedad es clave en darle su estructura a los logaritmos, y también es ampliamente utilizada en los algoritmos de antidiferenciación a discutirse más adelante. Lo mismo es cierto sobre la propiedad a continuación.

Propiedad 7.2: Sea F un campo diferencial con $f \in F$ y $f \neq 0$, y sea $n \in \mathbb{Z}$. Entonces,

$$\log(f^n) = n \log(f). \tag{7.2}$$

Demostración. Sea $\theta = \log(f^n)$. Entonces, por definición 7.1 y por propiedad 6.4,

$$D(\theta) = \frac{D(f^n)}{f^n} = \frac{nf^{n-1}D(f)}{f^n} = n\frac{D(f)}{f} = D(n \log(f)).$$

De nuevo, es gracias a la cancelación del operador diferencial que $\log(f^n) = n \log(f)$.

■

El logaritmo es, probablemente, la más importante de las funciones a definirse para trabajar en esta teoría. Sin embargo, es necesario definir a dos familias de funciones más. Aunque haremos uso de los siguientes tipos de funciones hasta dentro de un par de capítulos, será beneficioso mencionarlas desde ya. Empezamos con una función muy relacionada al logaritmo.

Definición 7.2: Sea F un campo diferencial, y sea G una extensión diferencial de F. Sea $g \in G$ tal que existe $f \in F$ que cumple la ecuación diferencial

$$D(g) = gD(f).$$

Entonces, se dice que g es un *exponencial* sobre F. Esto se denota por $g = \exp(f) = e^f$.

Nótese la similitud de la definición 7.2 de la exponencial con la definición 7.1 para el logaritmo. Esto no debería ser sorpresa, dado que es un hecho conocido que estas son funciones inversas. En efecto, es claro de las definiciones que $g = \exp(f)$ si y solo si $f = \log(g)$, considerando siempre el campo diferencial adecuado. Mostramos algunas de las propiedades esperadas de las funciones exponenciales.

Propiedad 7.3: Sea F un campo diferencial con $f, g \in F$. Entonces,

$$\exp(f + g) = \exp(f) \exp(g).$$

Demostración. Considérese $\theta = \exp(f) \exp(g)$. Luego,

$$\begin{aligned} D(\theta) &= D(\exp(f) \exp(g)) \\ &= \exp(f) D(\exp(g)) + \exp(g) D(\exp(f)) \\ &= \exp(f) \exp(g) D(g) + \exp(g) \exp(f) D(f) \\ &= \exp(f) \exp(g) D(f + g). \end{aligned}$$

Entonces, θ es exponencial sobre F, pues existe la función $f + g \in F$ tal que

$$D(\theta) = \theta D(f + g).$$

Haciendo uso de la notación, esto implica que $\theta = \exp(f + g)$. ■

Esta propiedad es análoga a la propiedad de suma de logaritmos. Ahora, demostramos la propiedad análoga a la del logaritmo de una potencia.

Propiedad 7.4: Sea F un campo diferencial con $f \in F$, y sea $n \in \mathbb{Z}$. Entonces,

$$\exp(f)^n = \exp(nf).$$

Demostración. Sea $\theta = \exp(f)^n$. Luego,

$$\frac{D(\theta)}{\theta} = \frac{D(\exp(f)^n)}{\exp(f)^n} = \frac{n \exp(f)^{n-1} D(\exp(f))}{\exp(f)^n} = n \frac{D(\exp(f))}{\exp(f)} = nD(f) = D(nf).$$

Haciendo uso de la notación para exponenciales, esto produce $\theta = \exp(nf)$. ■

Estas son las propiedades algebraicas más importantes de las funciones exponenciales. Más adelante, se hará uso de ellas para pensar en las propiedades diferenciales de dichas funciones. En este momento, nos movemos a definir el último tipo de función elemental.

Supóngase que se desea definir algebraicamente a la función radical $g = \sqrt[n]{x}$. Podría empezarse por notar que $g^n - x = 0$; esto es, existe un polinomio $p \in F[z]$ tal que $p(g) = 0$, dado por la regla de asignación $p(z) = z^n - x$. Aquí x es visto como un elemento de F y puede ser visto entonces como un coeficiente de un polinomio en $F[z]$. Esta es la intuición detrás de la siguiente definición, la cual reciben las funciones algebraicas.

Definición 7.3: Sea F un campo diferencial que contiene al símbolo x, y sea G una extensión diferencial de F. Sea $g \in G$ para la cual existe un polinomio $p \in F[z]$ tal que

$$p(g) = 0.$$

Entonces, se dice que g es *algebraica* sobre F.

Como complemento a lo que se observó en la discusión previa, las funciones radicales en la forma $g = \sqrt[n]{f}$ para $f \in F$ son algebraicas sobre F debido a que $g^n - f = 0$ satisface al polinomio $p(z) = z^n - f \in F[z]$. Esto además implica que cualquier combinación de campo entre funciones radicales es una función algebraica, pues es conocido que los elementos algebraicos sobre un campo F forman un campo de extensión (véase el capítulo 5 del libro de Herstein [12]).

Nota Bene 7.1: Sobre las funciones algebraicas.

Aunque todas las combinaciones de campo que puedan surgir de funciones radicales son parte de las funciones algebraicas, estas no son las únicas posibles funciones algebraicas que existen. Esto es una consecuencia directa del teorema de imposibilidad de Abel para solucionar de forma general un polinomio de grado mayor o igual a 5. Si uno considera un polinomio como $p(z) = z^5 - z - x$, resulta que $p(g) = 0$ no es una ecuación que pueda solucionarse para g en radicales, aunque una función g sí pueda existir.

De la misma manera que el polinomio $x^5 - x - 1$ posee 5 raíces complejas, puede que existan varias funciones tales que $g^5 - g - x = 0$, aunque no sean expresables en términos de combinaciones de campo y radicales. Este hecho puede observarse en la figura a continuación.

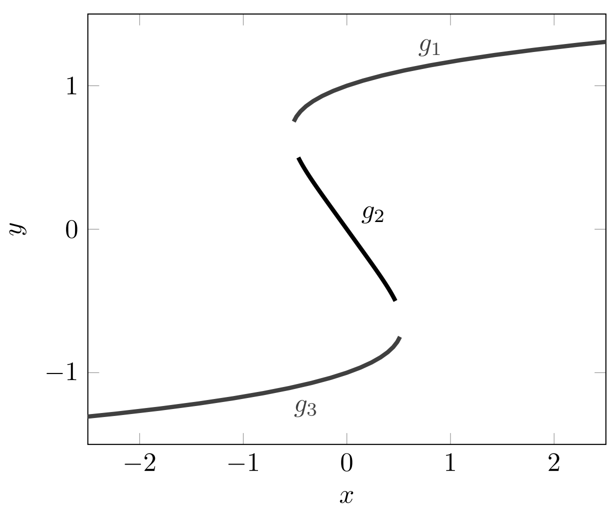

Figura 7.1: Tres funciones que cumplen la relación $y^5 - y - x = 0$.

Es claro entonces que funciones de este tipo existen, y al ser polinomios con los ejes rotados también es posible observar que son integrables por intervalos, de manera que considerar su antiderivada tiene sentido. Además, estas funciones presentan propiedades deseables en el análisis. Por ejemplo, el libro de análisis complejo de Ahlfors [1] demuestra que toda función algebraica es analítica, haciendo uso del principio del argumento de Cauchy.

Antes de finalizar nuestra discusión sobre la antidiferenciación de funciones, reconocemos la utilidad de pensar en el concepto opuesto a la función algebraica. Es por ello que definimos a las funciones trascendentales.

Definición 7.4: Sea F un campo diferencial que contiene al símbolo x, y sea G una extensión diferencial de F. Sea $g \in G$ tal que no es algebraica sobre F. Entonces, se dice que g es *trascendental* sobre F.

Cabe resaltar que los cuatro tipos de funciones aquí definidos no necesariamente son independientes entre sí. Por ejemplo, si se considera a la función $g = \exp\left(\frac{x}{2}\right)$ respecto a un campo diferencial $F = K(x, \exp(x))$, es inmediato pensar en g como una función exponencial sobre F. Pero también es posible observar que $g^2 - \exp(x) = 0$, de manera que g satisface al polinomio $p(z) = z^2 - \exp(x) \in F[z]$. Por lo tanto, g es tanto exponencial como algebraica sobre F.

7.1.2. Estructura de las funciones elementales

Se han definido previamente todas las piezas que nos permiten hablar de funciones elementales. Con ello, es posible hablar de las extensiones elementales de campo, y definir formalmente al concepto de *función elemental*.

Definición 7.5: Sea F un campo diferencial, y sea G una extensión diferencial de F. Se dice que G es una *extensión elemental* de F si es de la forma

$$G = F(g_1, g_2, \ldots, g_n),$$

donde para cada índice $1 \leq k \leq n$ se tiene que g_k es logarítmica, exponencial o algebraica sobre el campo $F_{k-1} = F(g_1, g_2, \ldots, g_{k-1})$. Cuando ninguna extensión es algebraica, se dice que G es una *extensión elemental trascendental*. Aquí, se toma $F_0 = F$.

Es importante notar que la diferencia entre las extensiones elementales y las extensiones elementales trascendentales es que la segunda elimina la posibilidad de que una extensión sea algebraica. Las extensiones trascendentales suelen ser más fáciles de trabajar que las algebraicas, en lo que concierne a la integración simbólica, y los métodos y demostraciones sobre antiderivadas elementales son muy distintos dependiendo de los tipos de funciones a integrar. Resulta que el caso que requiere más maquinaria algebraica es, quizá no tan irónicamente, el de las funciones algebraicas. Esto se debe a que la manipulación de las funciones trascendentales se comporta de una manera más estructurada que las funciones algebraicas, por lo general.

La última definición no es contundente en cuanto a qué es exactamente una función elemental, pues hay mucha libertad sobre el campo diferencial F. Nuestro interés es que las funciones elementales sean funciones de una sola variable, que puedan aparecer en el interior de un integrando. Es por ello que se usa como campo base a $F = K(x)$ en la definición siguiente.

Definición 7.6: Sea $K(x)$ un campo diferencial, donde K es un subcampo de $\mathbb{C}$. Se dice que G es un *campo de funciones elementales* si es una extensión elemental de $K(x)$. Si además G es una extensión trascendental sobre $K(x)$, entonces es un *campo de funciones elementales trascendentales*. De esta manera, una función es una *función elemental* si pertenece a un campo de funciones elementales.

Nos interesa conocer el comportamiento de las funciones elementales, y será importante reconocer la forma más simple que puede presentar una función elemental trascendental. Para ello, se requiere la siguiente definición.

Definición 7.7: Sea F un campo diferencial. Se dice que una función g es un *monomio* sobre F si cumple lo siguiente:

- $\mathrm{con}\big(F(g)\big) = \mathrm{con}(F)$.
- g es trascendental sobre F.
- g es exponencial o logarítmica sobre F.

Con esta definición, lo que interesará será determinar bajo qué circunstancias una función g que se desee integrar simbólicamente será un monomio. O bien, se desea reconocer cuándo una función g es un monomio sobre el campo diferencial F. Esto, en busca de simplificar las expresiones algebraicas lo más posible para facilitar el proceso de integración.

En 1979, Risch [18] demostró el teorema de estructura de las funciones elementales, el cual proporciona las condiciones necesarias que debe cumplir una función en una extensión para ser un monomio nuevo, dando una noción de independencia entre las posible extensiones elementales. Esto traduce el problema a un simple sistema de ecuaciones lineales, cuya solución es extraíble de manera algorítmica. Como se mencionó al inicio de este capítulo, la demostración de este teorema se sale de un enfoque de licenciatura, por lo cual se refiere al lector a la demostración propuesta por Risch.

Teorema 7.1 (Risch, Estructura de las funciones elementales)**:** Sea K un subcampo de $\mathbb{C}$, y sea $F_n = K(x, g_1, g_2, \ldots, g_n)$ una extensión de $K(x)$ tal que $\mathrm{con}(F_n) = K$. Además, supóngase que cada g_k es uno de las siguientes:

- Algebraico sobre F_{k-1}.
- Un logaritmo $w_k = \log(u_k)$ con $u_k \in F_{k-1}$.
- Un exponencial $u_k = \exp(w_k)$ con $w_k \in F_{k-1}$

Entonces, se cumple que:

- La función $g = \log(f)$ con $f \in F_n - K$ es un monomio sobre F_n si y solo si no existe una combinación en producto de la forma
$$h = f^n \prod_{k=1}^{m} u_k^{n_k} \in K,$$
donde n y n_k son enteros con $n \neq 0$.
- La función $f = \exp(g)$ con $g \in F_n - K$ es un monomio sobre F_n si y solo si no existe una combinación lineal de la forma
$$c = g - \sum_{k=1}^{m} c_k w_k \in K,$$
donde $c_k \in \mathbb{Q}$ para cada subíndice k.

Este teorema tiene varias aplicaciones importantes, las cuales también son discutidas en el artículo de Risch. Entre ellas están: determinar bajo qué condiciones dos elementos en un campo diferencial son distintos, encontrar campos elementales de extensión intermedios, evitar trabajar con números complejos a través de campos diferenciales elementales reales, y encontrar funciones inversas para las funciones elementales.

La aplicación que más nos interesa en este momento es determinar si una función exponencial o logarítmica sobre un campo es algebraicamente independiente de las demás funciones en el campo diferencial. Esto siempre puede traducirse a un problema de álgebra lineal, que puede resolverse con técnicas computacionales.

Dada una función de extensión exponencial $\exp(g)$, únicamente es necesario chequear si su argumento puede ser escrito como $g = c + \sum_{k=1}^{m} c_k w_k$, donde $c \in F$ y cada $c_k \in \mathbb{Q}$. Diferenciando esto, se obtiene un sistema de ecuaciones lineales con variables c_k. Al obtener sus valores, es posible obtener c.

Si por otro lado se nos da una función de extensión logarítmica $\log(f)$, el teorema muestra que el chequeo puede realizarse escribiendo $h = f^n \prod_{k=1}^{m} u_k^{n_k}$ para enteros n y n_k, e igualando $h' = 0$ de manera que $h \in K$. Como es claro que

$$\log(h) = n \log(f) + \sum_{k=1}^{m} n_k \log(u_k),$$

entonces diferenciando esta ecuación se tendría que

$$0 = \frac{h'}{h} = n\frac{f'}{f} + \sum_{k=1}^{m} n_k \frac{u_k'}{u_k}.$$

El problema se convierte en determinar si esta ecuación tiene soluciones en los n_k y n, provocando de nuevo que su solución pueda transformarse en resolver un sistema de ecuaciones lineales.

El algoritmo proveniente de este teorema permite optimizar la búsqueda del campo diferencial que contiene al integrando, de manera que no haya redundancia en las funciones de extensión escogidas. Además, proporciona una idea intuitiva detrás de la forma que puede tener un monomio logarítmico o exponencial, lo cual cobrará importancia en los teoremas de diferenciación e integración de funciones elementales con términos exponenciales.

7.2. Diferenciación de funciones elementales

Habiendo definido de manera exacta lo que es un campo de funciones elementales, y con el teorema de estructura de Risch, es posible encontrar las propiedades diferenciales de las funciones elementales. Pero además, también poseemos la capacidad de definir formalmente el problema a resolver dentro de la integración simbólica. Como punto importante, a partir de esta sección se reemplazará el uso del operador diferencial $D : F \to F$ por el más conveniente $' : F \to F$. Es decir, se tomará $D(f) = f'$ para todo $f \in F$.

Nota Bene 7.2: Enunciado formal del problema de integración simbólica.

Dada una función f, miembro de un campo de funciones elementales $F = K(x, g_1, g_2, \ldots, g_n)$, se desea encontrar una función $g = \int f$ que sea miembro de un campo de extensión elemental de F, dado por $G = F(g_{n+1}, g_{n+2}, \ldots, g_{n+m}) = K(x, g_1, g_2, \ldots, g_{n+m})$. Dicho problema se consideraría resuelto en uno de dos casos:

- Se logra determinar explícitamente a la función g como un elemento de G. Es decir, se demuestra que existe una extensión elemental G que contiene a g.
- Se logra demostrar que no existe ninguna extensión elemental G de F que contenga a g y que cumpla con los requerimientos establecidos.

Resulta claro, de esta manera, que lo que se requiere para un procedimiento de decisión que resuelva el problema para cualquier f son dos cosas: un algoritmo de solución simbólica para antiderivadas, y en caso dicha solución no exista, una manera de demostrarlo formalmente. Para cualquiera de estas dos, es necesario conocer la forma que debería poseer una integral de una función elemental. Es por esto que el siguiente tema a discutir es el comportamiento que posee el operador diferencial en las funciones elementales.

A continuación, se demuestran varios teoremas sobre las derivadas de funciones elementales. Es suficiente considerar por separado tres casos: logarítmico, exponencial y algebraico.

Teorema 7.2: Sea F un campo diferencial con el símbolo x, y sea $F(g)$ una extensión diferencial de F tal que $\operatorname{con}(F) = \operatorname{con}(F(g))$ Supóngase que g es logarítmica y trascendental sobre F, tomando $g = \log(f)$ para un $f \in F$. Entonces, para todo $a(g) \in F[g]$ con $\deg(a(g)) > 0$ se cumple que:

- $[a(g)]' \in F[g]$.
- Si el coeficiente principal de $a(g)$ es una constante en F, entonces $\deg([a(g)]') = \deg(a(g)) - 1$.
- Si el coeficiente principal de $a(g)$ no es una constante en F, entonces $\deg([a(g)]') = \deg(a(g))$.

Demostración. Escríbase $a(g) = \sum_{k=0}^{n} a_k g^k$, donde los $a_k \in F$ son coeficientes posiblemente no constantes y $a_n \neq 0$. Luego,

$$\begin{aligned}
[a(g)]' = \left(\sum_{k=0}^{n} a_k g^k\right)' &= \sum_{k=0}^{n} (a_k' g^k + k g^{k-1} g' a_k) \\
&= \sum_{k=0}^{n} a_k' g^k + \sum_{k=0}^{n-1} (k+1) g^k g' a_{k+1} \\
&= a_n' g^n + \sum_{k=0}^{n-1} (a_k' + (k+1) g' a_{k+1}) g^k. \qquad (7.3)
\end{aligned}$$

Nótese además que dado $g = \log(f)$, entonces $g' = f'/f \in F$. Puesto que la expresión obtenida para $[a(g)]'$ es una combinación de operaciones de campo en elementos de F multiplicadas por potencias enteras no negativas de g, esto implica que $[a(g)]' \in F[g]$, demostrando el primer resultado deseado.

Supóngase ahora que el coeficiente principal de $a(g)$ es una constante en F, teniendo entonces $a_n' = 0$. Desde luego, observando la ecuación 7.3, esto implicaría que $\deg([a(g)]') \leq n - 1$. Por vía de contradicción, tomemos que $\deg([a(g)]') < n - 1$. Esto implicaría que el coeficiente de g^{n-1} se anularía, produciendo la ecuación $a_{n-1}' + n g' a_n = 0$. Considérese al elemento $n a_n g + a_{n-1} \in F(g)$. Nótese que:

$$(n a_n g + a_{n-1})' = n a_n' g + n a_n g' + a_{n-1}'.$$

Pero $a_n' = 0$ y $n a_n g' + a_{n-1}' = 0$. Entonces, $n a_n g + a_{n-1}$ es una constante en $F(g)$. Sin embargo $\operatorname{con}(F) = \operatorname{con}(F(g))$, implicando que $n a_n g + a_{n-1} \in F$. Puesto que g es trascendental sobre F, esto es absurdo. Por tanto, es necesario que $\deg([a(g)]') = n - 1 = \deg(a(g)) - 1$, como se requería en el segundo punto.

Finalmente, supóngase que el coeficiente principal de $a(g)$ no es constante, provocando que $a_n' \neq 0$. De la ecuación 7.3, esto implica directamente que la potencia mayor de $[a(g)]'$ sea exactamente igual a la de $a(g)$. Es decir, $\deg([a(g)]') = \deg(a(g)) = n$, demostrando el enunciado del tercer punto.

■

Como pudo observarse en la demostración, la derivada de cualquier polinomio logarítmico resulta en otro polinomio logarítmico, pero el grado de este nuevo polinomio depende de si el coeficiente principal del polinomio original era una constante. Mientras en los polinomios exponenciales se preserva la cerradura en el anillo de polinomios, el grado del polinomio nuevo será independiente del coeficiente principal. Además, se agregan dos propiedades nuevas, pertinentes a los monomios exponenciales.

Teorema 7.3: Sea F un campo diferencial con el símbolo x, y sea $F(g)$ una extensión diferencial de F tal que $\text{con}(F) = \text{con}(F(g))$ Supóngase que g es exponencial y trascendental sobre F, tomando $g = \exp(f)$ para un $f \in F$. Entonces, para todo $a(g) \in F[g]$ con $\deg(a(g)) > 0$ se cumple que:

- Si $h \in F$ y $n \in \mathbb{Z}$ son no nulos, entonces $(hg^n)' = \bar{h}g^n$ para un $\bar{h} \in F$ no nulo.
- $[a(g)]' \in F[g]$ y $\deg([a(g)]') = \deg(a(g))$.
- $a(g) \mid [a(g)]'$ si y solo si $a(g)$ es un monomio.

Demostración. Como primera observación, nótese que:

$$(hg^n)' = h'g^n + ng^{n-1}g'h = (h' + nh \cdot g'/g)g^n = (h' + nhf')g^n.$$

De esta manera, se tiene la forma deseada en el primer punto, y únicamente queda demostrar que $\bar{h} = h' + nhf'$ es no nulo. Supóngase entonces que $\bar{h} = 0$. Esto implicaría que $(hg^n)' = 0$, y por lo tanto $hg^n \in \text{con}(F(g)) = \text{con}(F) \subseteq F$. Pero g es trascendental sobre F, por lo cual esto es imposible. Entonces $\bar{h} \neq 0$, demostrando el primer punto.

Ahora, escríbase $a(g) = \sum_{k=0}^{n} a_k g^k$, donde los $a_k \in F$ son coeficientes posiblemente no constantes y $a_n \neq 0$. Por lo tanto, del resultado anterior, se tendrá que

$$[a(g)]' = \sum_{k=0}^{n} \bar{a_k} g^k,$$

para $\bar{a_n} \in F$ no nulo. Con esto, se tiene directamente que $[a(g)]' \in F[g]$ y $\deg([a(g)]') = \deg(a(g))$, como se buscaba en el segundo punto.

Para demostrar el tercer punto, supóngase primero que $a(g)$ es un monomio. Entonces, debe poseer la forma $a(g) = hg^n$ para un $h \in F$ y un $n \in \mathbb{Z}$ debido al teorema 7.1 de estructura de Risch. Directamente se sigue por lo demostrado en la primera propiedad que

$$\frac{[a(g)]'}{a(g)} = \frac{h'}{h} + nf' \in F,$$

puesto que $h, h', f' \in F$. Esto es, $a(g)$ divide a $[a(g)]'$ en $F[g]$, demostrando la condición suficiente del punto tres.

Únicamente queda por demostrar la condición necesaria del último punto. Para ello, tomemos que $a(g) \mid [a(g)]'$ en $F[g]$, y supóngase que $a(g)$ no es monomio en busca de una contradicción. Luego, para algún $u \in F[g]$ se tiene que $[a(g)]' = ua(g)$. Pero dado que $\deg(a(g)) = \deg([a(g)]')$, es imposible que u dependa de g, por lo cual $u \in F$. Ahora, dado que $a(g)$ no es monomio, debe ocurrir que exista un entero $m < \deg(a(g))$ para el cual aparezca el término g^m en la expansión de $a(g)$. De esta manera, al factorizar la máxima potencia posible de g en la expansión de $a(g)$, lo restante dependerá de g, quitando la posibilidad de que $a(g)$ sea monomio. Escríbase entonces

$$a(g) = a_n g^n + a_m g^m + b(g), \tag{7.4}$$

donde además $m > 0$, $a_m \neq 0$, y $\deg(b(g)) < m$, sin eliminar la posibilidad de que $b(g) = 0$.

Como nota importante, la razón por la cual $m \neq 0$ es que si se diera $a(g) = a_n g^n + a_0$, entonces $[a(g)]' = \bar{a_n} g^n + a_0'$ con $\bar{a_n} \neq 0$, pero existe la posibilidad de que $a_0' = 0$. Dado que $[a(g)]' = ua(g)$, se tendría entonces $\bar{a_n} g^n = u a_n g^n + u a_0$, lo cual implica que $u a_0 = (\bar{a_n} - u a_n) g^n$. Como $u a_0 \in F$ y g es trascendental sobre F, esto solo podría ocurrir si $u a_0 = 0$ y $\bar{a_n} - u a_0 = 0$, mas esto es imposible dado que $\bar{a_n} \neq 0$, $a_0 \neq 0$ y $u \neq 0$, de manera que se vuelve necesario $m > 0$.

Prosiguiendo, de diferenciar la ecuación 7.4 se obtiene que

$$[a(g)]' = \bar{a_n} g^n + \bar{a_m} g^m + [b(g)]',$$

donde $\bar{a_n} \neq 0$ y $\bar{a_m} \neq 0$. Además, por la segunda propiedad ya demostrada, se mantiene que $\deg([b(g)]') < m$. De nuevo gracias a que $[a(g)]' = u a(g)$, y recordando que $\bar{a_k} = a_k' + k a_k f'$ como se vio en la prueba de la primera propiedad, se implica que

$$(a_n' + n a_n f') g^n + (a_m' + m a_m f') g^m + [b(g)]' = u(a_n g^n + a_m g^m + b(g)).$$

Esto nos lleva a las siguientes dos ecuaciones:

$$\begin{aligned} a_n' + n a_n f' &= u a_n, \\ a_m' + m a_m f' &= u a_m. \end{aligned}$$

Resolviendo el sistema mediante igualación en u, se llega a

$$\frac{a_m' + m a_m f'}{a_m} = \frac{a_n' + n a_n f'}{a_n} \implies \frac{a_n'}{a_n} - \frac{a_m'}{a_m} + (n-m) f' = 0.$$

Como último paso, se considera al elemento $\frac{a_n}{a_m} g^{n-m} \in F[g]$. Al diferenciarlo, se obtiene

$$\begin{aligned} \left(\frac{a_n}{a_m} g^{n-m} \right)' &= \frac{a_n' a_m - a_n a_m'}{a_m^2} g^{n-m} + \frac{a_n}{a_m} (n-m) g^{n-m-1} g' \\ &= \frac{a_n}{a_m} g^{n-m} \left(\frac{a_n'}{a_n} - \frac{a_m'}{a_m} + (n-m) f' \right) = 0. \end{aligned}$$

Esto implicaría que $\frac{a_n}{a_m} g^{n-m}$ es constante en $F(g)$, lo cual implica que es constante en F, y por lo tanto $\frac{a_n}{a_m} g^{n-m} \in F$. Esto es absurdo porque g es trascendental sobre F. Así, se llega a que $a(g)$ debe ser un monomio, demostrando finalmente el tercer resultado.

■

Esta demostración requirió bastante más trabajo que la del teorema 7.2, pero también proporcionó bastantes más propiedades a la diferenciación de polinomios exponenciales. Sin embargo, dichas propiedades provocarán que los teoremas de integración de funciones exponenciales sean ligeramente más complicados que los de funciones logarítmicas, lo cual se discutirá en el capítulo 10. Por ahora, continuamos con el teorema de diferenciación de polinomios con entradas algebraicas, el cual difiere bastante de los dos anteriores.

Teorema 7.4: Sea F un campo diferencial con el símbolo x, y sea $F(g)$ una extensión diferencial de F tal que $\text{con}(F) = \text{con}(F(g))$. Supóngase que g es algebraica sobre F, tomando a $p \in F[z]$ como el polinomio mínimo tal que $p(g) = 0$. Escríbase este polinomio como $p(z) = \sum_{k=0}^{N+1} p_k z^k$, donde $N \geq 0$ y $p_{N+1} = 1$ de manera que p sea mónico. Entonces, g' puede expresarse como

$$g' = -\frac{\sum_{k=0}^{N} p_k' g^k}{\sum_{k=0}^{N} (k+1) p_{k+1} g^k} \in F(g). \tag{7.5}$$

Demostración. Como $p(g) = 0$, entonces se tiene $\sum_{k=0}^{N+1} p_k g^k = 0$. Diferenciando ambos lados de esta igualdad,

$$\sum_{k=0}^{N+1} (p_k' g^k + k p_k g^{k-1} g') = 0 \implies g' \sum_{k=0}^{N} (k+1) p_{k+1} g^k = -\sum_{k=0}^{N+1} p_k' g^k.$$

Además, en el lado derecho, $p'_{N+1} = 0$. Por tanto, a partir de aquí, el resultado es inmediato:

$$g' = -\frac{\sum_{k=0}^{N} p'_k g^k}{\sum_{k=0}^{N} (k+1) p_{k+1} g^k} \in F(g).$$

Esta expresión nunca se indefine, gracias a que el denominador tiene coeficiente principal $N+1 \geq 1$. Por lo tanto, el denominador es una función no nula.

■

Con estos tres teoremas sobre la estructura diferencial de las funciones elementales, estamos listos para entrar de lleno a la discusión principal de este trabajo: los algoritmos de integración de funciones elementales. Antes de ello, es necesario hablar de la existencia y unicidad del operador diferencial en una nueva extensión de un campo de funciones elementales. La prueba que se presentará va por casos sobre los tipos de funciones elementales, pero una prueba para campos diferenciales completamente generales puede encontrarse en el artículo de Rosenlicht [20].

Propiedad 7.5: Sea F un campo diferencial. Entonces:

- **Caso logarítmico:** Si g es trascendental sobre F y $u \in F$, existe una única manera de extender el operador diferencial $' : F \to F$ al campo de extensión $F(g)$ de manera que $g' = u'/u$.
- **Caso exponencial:** Si g es trascendental sobre F y $u \in F$, existe una única manera de extender el operador diferencial $' : F \to F$ al campo de extensión $F(g)$ de manera que $g' = u'g$.
- **Caso algebraico:** Si g es algebraico sobre F, existe una única manera de extender el operador diferencial $' : F \to F$ al campo de extensión $F(g)$. En particular, el operador diferencial en $F(g)$ está completamente determinado por el polinomio mínimo de $F[z]$ que satisface a g, y por el operador diferencial de F.

Como consecuencia, dado un campo F con operador diferencial $' : F \to F$, entonces una extensión elemental G de F siempre posee una única extensión del operador diferencial, denotada $' : G \to G$.

Demostración. Las pruebas de todos los casos proceden por construcción, y una buena parte de las construcciones proviene de los teoremas de diferenciación. En general, la estrategia es notar que $F(g)$ es el campo de las funciones racionales sobre g con coeficientes en F, de manera que únicamente es necesario demostrar que si se define una manera de diferenciar g, entonces también se posee una manera de diferenciar cualquier función racional en g sobre F.

Para el caso logarítmico, sea F un campo, sea $u \in F$ y sea g trascendental sobre F. Considérese a un nuevo operador diferencial $' : F(g) \to F(g)$ con la propiedad de que $g' = u'/u$, y que restricto a F es igual al operador $' : F \to F$. Sea $a(g) \in F[g]$, escribiéndolo como $a(g) = \sum_{k=0}^{n} a_k g^k$ para $a_k \in F$. Entonces, como se vio en el teorema 7.2, puede determinarse por completo la derivada de $a(g)$ como en la ecuación 7.3 a través de

$$[a(g)]' = \left(\sum_{k=0}^{n} a_k g^k\right)' = a'_n g^n + \sum_{k=0}^{n-1} \left(a'_k + \frac{(k+1)u' a_{k+1}}{u}\right) g^k.$$

Esto implica que, dado cualquier polinomio en g sobre F, el operador aplicado al mismo está determinado por completo, de manera que hay una única manera de extender $' : F \to F$ a $' : F[g] \to F[g]$. Ahora bien, considérese una función racional $p(g)/q(g) \in F(g)$, para la cual escribimos $p(g) = \sum_{k=0}^{m} p_k g^k$ y $q(g) = \sum_{k=0}^{n} q_k g^k$, donde $p_k, q_k \in F$. Por la regla del cociente,

$$\left[\frac{p(g)}{q(g)}\right]' = \frac{q(g)[p(g)]' - p(g)[q(g)]'}{[q(g)]^2}.$$

Pero como $[p(g)]'$ y $[q(g)]'$ están completamente determinados, se tiene así que la derivada de todo elemento de $F(g)$ también lo está. Es decir, existe un único operador diferencial que extiende al operador en F al campo diferencial $F(g)$, de manera que g sea logarítmico trascendental sobre F.

Para el caso exponencial, aplica el mismo argumento. Si $g' = gu'$ para $u \in F$, entonces un polinomio $a(g) \in F[g]$ con coeficientes $a_k \in F$ cumplirá necesariamente

$$[a(g)]' = \left(\sum_{k=0}^{n} a_k g^k\right)' = a_0' + \sum_{k=1}^{n}(a_k' + ku'a_k)g^k.$$

De aquí, se tiene la extensión $' : F[g] \to F[g]$. Para fabricar la extensión en $F(g)$, el argumento no presenta cambio alguno con respecto al caso anterior. Esto culmina el caso exponencial.

Finalmente, es necesario considerar el caso algebraico. Sea g algebraica sobre F, y sea $p(z) = \sum_{k=0}^{N+1} p_k z^k \in F[z]$ el polinomio mónico mínimo tal que $p(g) = 0$. Por la argumentación del teorema 7.4 resulta necesario que se asigne la derivada siguiente a g:

$$g' = -\frac{\sum_{k=0}^{N} p_k' g^k}{\sum_{k=0}^{N}(k+1)p_{k+1}g^k} \in F(g).$$

Sea ahora $a(g) \in F[g]$ con $a(g) = \sum_{k=0}^{n} a_k g^k$, de lo cual

$$[a(g)]' = \sum_{k=0}^{n}(a_k' g^k + ka_k g^{k-1}g') = \sum_{k=0}^{n}\left(a_k' g^k - ka_k g^{k-1}\frac{\sum_{j=0}^{N} p_j' g^j}{\sum_{j=0}^{N}(j+1)p_{j+1}g^j}\right).$$

Con esto, la derivada de todo polinomio en $F[g]$ está determinada de manera única. Por el mismo argumento a través de la regla del cociente, esto implica que $' : F(g) \to F(g)$ existe y es único.

En general, si F es un campo diferencial, y G es una extensión elemental de F, entonces el operador diferencial en F puede extenderse de manera única al operador diferencial $' : G \to G$.

■

Esto cubre por completo las propiedades algebraicas y diferenciales necesarias para demostrar el resto de la teoría a estudiarse en la presente investigación. Aunque los casos más simples de integración simbólica no requieren de todas las herramientas aquí planteadas, al adentrarnos más en la teoría será necesario utilizar cada vez más de estos conceptos.

CAPÍTULO 8

Algoritmos de integración de funciones racionales

En un curso de cálculo resulta claro que los problemas de integración son, por lo general, muy distintos uno del otro. Normalmente, en estos cursos, se estudian varios métodos y técnicas diferentes para resolver integrales con formas muy distintas. En esta observación radica una de las grandes dificultades para decidir si una función posee, o no, una antiderivada expresable en términos de funciones conocidas. ¿Cómo sería posible crear un algoritmo de decisión, si no se posee un algoritmo de solución?

Sin embargo, existe una familia de funciones para las cuales la solución sí parece ser algorítmica. De hecho, se trata de una familia de funciones ya discutida en un anterior capítulo de esta tesis: las funciones racionales. Considérese una integral como la que se muestra a continuación:

$$\int \frac{x^3 + 2x^2 - x + 1}{x^2 + 3x + 2}\, \mathrm{d}x \tag{8.1}$$

El primer paso a realizar en una integral como esta es el algoritmo de la división. Con esto, la integral se separa en dos partes: una polinómica, y una racional con grado mayor en el denominador. La integral de la parte polinómica es sencilla, como se vio en la propiedad 6.14. La integral de la parte racional requiere inspección, pero por lo regular, se realizaría uno de dos métodos: completación de cuadrados para llegar a una sustitución trigonométrica, o fracciones parciales.

Como se puede observar en la Nota Bene 6.4 y en el ejemplo 6.2, los dos procesos mencionados llevan a la integral a soluciones equivalentes. En efecto, cualquier integral de este tipo resulta en una combinación de polinomios, funciones racionales, logaritmos, y funciones trigonométricas inversas. Sin embargo, como se observa en el Anexo 14.1, estas últimas funciones pueden ser expresadas como logaritmos. Así, como se demostrará, únicamente será necesario agregar logaritmos a un campo diferencial de funciones racionales para expresar todas sus antiderivadas. Por lo tanto, más adelante, nos concentraremos sobre todo en el método que hace un uso más algorítmico de la herramienta algebraica: las fracciones parciales. Aunque a veces resultará necesario encontrar los ceros del polinomio en el denominador, vale la pena recordar que dicha tarea puede referirse a los métodos numéricos, y no debe ser preocupante en la integración simbólica.

8.1. Separación de la integral

La expresión 8.1 muestra un ejemplo de una integral de una función racional, y en la introducción de esta sección se sugiere un método algorítmico de resolución. Para motivar los algoritmos siguientes, resolvemos esta integral.

Ejemplo 8.1: Aplicando el algoritmo de la división, es posible separar esta función en dos partes:

$$\int \frac{x^3+2x^2-x+1}{x^2+3x+2}\,\mathrm{d}x = \int (x-1)\,\mathrm{d}x + \int \frac{3}{x^2+3x+2}\,\mathrm{d}x\,.$$

Con esto, la primera pieza de la integral se convierte en un polinomio fácil de integrar con la propiedad 6.14. La segunda pieza por lo general requiere un poco más de trabajo, pero en este caso podemos observar usando fracciones parciales que:

$$\int \frac{3}{x^2+3x+2}\,\mathrm{d}x = \int \left(\frac{3}{x+1} - \frac{3}{x+2}\right)\mathrm{d}x = 3\log(x+1) - 3\log(x+2).$$

Juntando esto con la integral del polinomio $x-1$, se tiene

$$\int \frac{x^3+2x^2-x+1}{x^2+3x+2}\,\mathrm{d}x = \frac{x^2}{2} - x + 3\log(x+1) - 3\log(x+2).$$

Como se observa muy transparentemente, existen dos partes clave en la resolución de una integral de este tipo. En primer lugar, se busca reducir la integral, separándola en distintas piezas. En el ejemplo, estas piezas toman una forma polinómica y una logarítmica, pero en general puede obtenerse una pieza racional y otra logarítmica. En segundo lugar, se busca realizar la integración simbólica. Más adelante, se observará que la pieza logarítmica es la que requiere más trabajo en cuanto a este segundo paso, en el caso general. Por ahora, se dirigirá el esfuerzo a encontrar una forma de separar la integral de una función racional en una pieza que sea completamente racional y otra que sea completamente logarítmica. Aunque existen varios algoritmos y estrategias de reducción que logran este cometido, nos enfocamos únicamente en el siguiente.

El teorema de reducción de Hermite

En 1872, Hermite [11] propuso un algoritmo que logra separar la antiderivada de cualquier función racional $p/q \in K(x)$ como

$$\int \frac{p(x)}{q(x)}\,\mathrm{d}x = \frac{c(x)}{d(x)} + \int \frac{a(x)}{b(x)}\,\mathrm{d}x\,, \tag{8.2}$$

donde $c/d, a/b \in K(x)$, con $\deg(a) < \deg(b)$ y b un polinomio mónico libre de cuadrados. Aquí, se toma a K como un campo de constantes respecto a x con característica 0.

En la forma de la ecuación 8.2, la expresión c/d es la parte racional de la integral, mientras que $\int a/b$ es la parte logarítmica de la integral. Se dará un algoritmo para su solución más adelante, pero por ahora nos enfocamos en demostrar que esto es posible.

Teorema 8.1 (Reducción de Hermite)**:** Sea $p/q \in K(x)$ una función racional simplificada de tal manera que q sea mónico y $(p,q)=1$. Entonces, existen funciones racionales $a/b, c/d \in K(x)$ con $\deg(a) < \deg(b)$ y b un polinomio mónico libre de cuadrados que cumplen la ecuación 8.2.

Únicamente resulta necesario considerar $p, q \in K[x]$ tales que q sea mónico y $(p,q)=1$ debido a que toda fracción algebraica puede ser llevada a esta forma a través de simplificaciones simples de fracciones. Nótese que este teorema únicamente busca mostrar la separación de la integral, mas no la forma de la antiderivada de a/b. El teorema de Rothstein-Trager se encargará del resto.

Demostración. Sean $p, q \in K[x]$ tales que q sea mónico y $(p, q) = 1$. Aplicando el algoritmo de la división a p/q, se sabe que existen $P, r \in K[x]$ con $r = 0$ o $\deg(r) < \deg(q)$ tales que $p = Pq + r$. Luego, es posible escribir

$$\int \frac{p}{q} = \int P + \int \frac{r}{q}.$$

Nótese que, al ser P un polinomio, su integración es trivial como se aprecia en la propiedad 6.14. Entonces, el problema se traduce a encontrar la antiderivada de r/q. Ahora, se procede a factorizar q en su forma libre de cuadrados. Desde luego, esto se realiza para reescribir la integral usando fracciones parciales. Así, tomando $q = \prod_{k=1}^{n} q_k^k$ con cada q_k mónico libre de cuadrados, se tiene

$$\int \frac{r}{q} = \int \frac{r}{\prod_{k=1}^{n} q_k^k} = \int \sum_{k=1}^{n} \left(\frac{r_{k_1}}{q_k} + \frac{r_{k_2}}{q_k^2} + \frac{r_{k_3}}{q_k^3} + \cdots + \frac{r_{k_k}}{q_k^k} \right) = \int \sum_{k=1}^{n} \sum_{j=1}^{k} \frac{r_{k_j}}{q_k^j} = \sum_{k=1}^{n} \sum_{j=1}^{k} \int \frac{r_{k_j}}{q_k^j}.$$

En esta forma, cada q_k tiene su separación en potencias $1 \leq j \leq k$, con numerador r_{k_j} cumpliendo $\deg(r_{k_j}) < \deg(q_k)$ para todo q_k no constante, o $r_{k_j} = 0$ si q_k es constante. La reorganización de la integral con las sumatorias está permitida por la linealidad del operador antidiferencial (propiedad 6.12), y debido a que se está trabajando con sumas finitas.

Ahora, el problema se reduce de nuevo, esta vez a encontrar un algoritmo de reducción para la integral de cada r_{k_j}/q_k^j. Esto se logra haciendo uso de la integración por partes (propiedad 6.13) y el algoritmo de la división. Obsérvese que, si $j = 1$, el sumando ya posee la forma deseada (denominador mónico, libre de cuadrados, con grado mayor al numerador). Considérese entonces un integrando arbitrario r_{k_j}/q_k^j con $j > 1$. Dado que q_k es libre de cuadrados, se tiene que $(q_k, q_k') = 1$. Esto implica por el lema de Bézout extendido (5.2) que existen $s, t \in K[x]$ tales que

$$sq_k + tq_k' = r_{k_j}, \tag{8.3}$$

donde $\deg(s) < \deg(q_k) - 1$ y $\deg(t) < \deg(q_k)$. Esto, a su vez, resulta en la ecuación integral

$$\int \frac{r_{k_j}}{q_k^j} = \int \frac{s}{q_k^{j-1}} + \int \frac{tq_k'}{q_k^j}. \tag{8.4}$$

La aparición de una derivada en el interior de la segunda integral sugiere el uso de integración por partes para simplificarla. Tomando $u(x) = t(x)$ y $v'(x) = q_k'(x)/q_k(x)^j$, entonces $u'(x) = t'(x)$ y $v(x) = q_k^{1-j}/(1-j)$. De esta manera,

$$\int \frac{tq_k'}{q_k^j} = -\frac{1}{j-1} \frac{t}{q_k^{j-1}} + \frac{1}{j-1} \int \frac{t'}{q_k^{j-1}}. \tag{8.5}$$

Juntando las ecuaciones 8.4 y 8.5, se obtiene:

$$\int \frac{r_{k_j}}{q_k^j} = -\frac{1}{j-1} \frac{t}{q_k^{j-1}} + \frac{1}{j-1} \int \frac{(j-1)s + t'}{q_k^{j-1}}.$$

Esto aporta a la parte racional de la integral con el primer término, y en el segundo término se obtiene una integral cuyo exponente en el denominador disminuyó en una unidad. Esto permite la entrada del proceso algorítmico, pues se puede realizar el mismo procedimiento varias veces hasta que $j - 1 = 1$. En ese caso, el denominador es mónico y libre de cuadrados, llegando a una integral con la forma deseada. Así, queda claro que es posible escribir la integral en una parte racional que será la combinación de la integral del polinomio P con la suma de todos los t/q_k^{j-1} restantes, más la suma de varias integrales con denominador mónico libre de cuadrados. Escrito de otra forma:

$$\int \frac{p}{q} = \left[\sum_{j,k} \frac{t_k}{q_k^{j-1}} + \int P \right] + \int \sum_{k=1}^{n} \frac{s_k}{q_k}. \tag{8.6}$$

En esta representación, $t_k \in K[x]$ son los numeradores de los resultados no integrales luego de realizar cada integración por partes, y $s_k \in K[x]$ son los numeradores de los resultados finales en la integral cuando $j-1=1$. De esta manera, dado que los q_k forman la factorización libre de cuadrados de q, el último integrando tendrá un denominador mónico y libre de cuadrados a la hora de tomar el denominador común, puesto que $(q_i(x), q_j(x)) = 1$ para todo $i \neq j$. Por construcción se debe tener también que $\deg(s_k) < \deg(q_k)$, de manera que la suma de los s_k/q_k debe tener también un numerador de grado menor al denominador. Con esto, dicho integrando es de la forma $a/b \in K(x)$, siendo b un polinomio mónico, libre de cuadrados, y $\deg(a) < \deg(b)$. Además, la expresión en corchetes claramente es una suma de elementos de $K(x)$, por lo cual es un elemento $c/d \in K(x)$. Con esto, queda demostrado el teorema de reducción de Hermite.

■

El algoritmo de Hermite no es la única forma de separar la integral en su parte racional y en su parte logarítmica. Existen otras perspectivas como la de Horowitz [13] y Mack [16]. La primera de estas utiliza el máximo común divisor para simplificar el cálculo de las integrales, mientras el segundo evita el uso de fracciones parciales en su proceso. En este trabajo, dado que el mayor interés es en las demostraciones de integrabilidad elemental, con uno de estos métodos es suficiente. A continuación, se muestra el algoritmo que nace del teorema 8.1.

Algoritmo 8.1: Reducción integral de Hermite.

1. Tomar una función racional $p_0/q_0 \in K(x)$ para K subcampo de $\mathbb{C}$.
2. Simplificar p_0/q_0 a p/q de tal manera que q sea mónico y $(p, q) = 1$.
3. Aplicar el algoritmo de la división, obteniendo una parte polinomial P y una parte racional escrita como r/q.
4. Calcular la factorización libre de cuadrados de q, resultando en una lista $q_1, q_2, \ldots, q_n$ de polinomios libres de cuadrados.
5. Con dicha factorización, calcular la descomposición en fracciones parciales de r/q, llegando a numeradores r_{k_j} para cada denominador q_k^j.
6. Inicializar la parte racional de la integral como $R = 0$ y la parte logarítmica de la integral como $L = 0$.
7. Se empieza un contador en $k = 1$, y terminará en $k = n$.
   - El valor de L se reemplaza por su valor anterior agregado a r_{k_1}/q_k.
   - Se inicializa el contador $j = 2$, y terminará en $j = k$.
     - Se reemplaza el valor de n por j.
     - Mientras que $n > 1$, se realiza lo siguiente:
       - Encontrar el valor de s y t que satisface $sq_k + tq_k' = r_{k_n}$.
       - Se reemplaza n por $n-1$.
       - El valor de R se reemplaza por su valor anterior menos $t/(nq_k^n)$.
       - Se reemplaza r_{k_n} por $s + t'/n$.
     - Se reemplaza L por su valor anterior más r_{k_1}/q_k. Se suma 1 al contador j.
   - Se suma 1 al contador k.
8. Regresar al usuario que la integral dada puede ser escrita en la forma $R + \int P + \int L$.

8.2. Integración simbólica de la pieza logarítmica

En la sección anterior, se provee un algoritmo que descompone la integral de una función racional general $p/q \in K(x)$ en una pieza racional $c/d \in K(x)$, y otra llamada logarítmica. La primera pieza es la función racional exacta que forma parte de la respuesta al problema de integración, mientras la segunda pieza aún permanece sin antidiferenciar. En esta sección, se demostrará que la antiderivada $\int a/b$ es una combinación lineal de logaritmos, y se proporcionará un algoritmo para calcularla.

Los teoremas de Rothstein-Trager

La idea en esta sección, como se evidenció en la discusión previa, es tomar una función racional como la que aparece en el integrando resultante del método de Hermite, para escribir su antiderivada en términos de funciones conocidas. Se ha discutido, también, que esto se puede lograr únicamente con una combinación lineal de logaritmos. Se empezará con un teorema que demuestra esta afirmación. Luego, se demostrará el teorema que da la forma final de la integral, y proveerá una estrategia de cálculo para la misma. Se continuará con un teorema que demuestra que el método dado utiliza el campo de adjunción de constantes mínimo, y finalmente se mostrará el algoritmo como tal.

Teorema 8.2 (Primer teorema de Rothstein-Trager para funciones racionales)**:** Sea $a/b \in K(x)$ sobre un campo K, tal que b es mónico, libre de cuadrados, y con $\deg(a) < \deg(b)$ y $(a, b) = 1$. Entonces, la integral $\int a/b$ puede ser expresada como una combinación lineal de logaritmos.

Demostración. Sea $a/b \in K(x)$ tal que b es mónico, libre de cuadrados, y con $\deg(a) < \deg(b)$. Como en la sección anterior, será deseable usar fracciones parciales para simplificar el integrando. Para ello, sea K_b el campo de descomposición de $b(x) \in K[x]$, y sean $\beta_k \in K_b$ las raíces de b. Luego, recordando que b es mónico, se tiene $b(x) = \prod_{k=1}^{m}(x - \beta_k)$. De esta manera, se puede escribir

$$\frac{a}{b} = \frac{a}{\prod_{k=1}^{m}(x - \beta_k)} = \sum_{k=1}^{m} \frac{\gamma_k}{x - \beta_k}. \tag{8.7}$$

Esto, con los $\gamma_k \in K_b$ provenientes del proceso de fracciones parciales para a/b. De aquí, se sigue usando las propiedades 6.12 y 6.11, y la definición 7.1, que:

$$\int \frac{a}{b} = \int \sum_{k=1}^{m} \frac{\gamma_k}{x - \beta_k} = \sum_{k=1}^{m} \gamma_k \int \frac{1}{x - \beta_k} = \sum_{k=1}^{m} \gamma_k \log(x - \beta_k).$$

■

Claramente, esta solución pertenece a la extensión $K_b(x, \log(x - \beta_1), \cdots, \log(x - \beta_m))$. Pero es un hecho conocido que obtener el campo de descomposición K_b puede ser computacionalmente demandante. Esto, debido a que si $K = \mathbb{Q}$ entonces el campo de descomposición K_b podría tener grado $\deg(b)!$, cuyo crecimiento es incluso más acelerado que uno exponencial. Sin embargo, no siempre es necesario utilizar el campo de descomposición para expresar la antiderivada.

Aunque nuestro objetivo no es encontrar el método de integración más rápido o práctico, en este momento resulta oportuno terminar de analizar el método de Rothstein-Trager, pues es deseable evitar el uso del campo de descomposición cuando sea posible. Esto será importante también al generalizar el algoritmo a la integración de funciones elementales más complicadas. El método de Rothstein-Trager se encargará de transformar el problema de encontrar los coeficientes γ_k y los polinomios dentro de los logaritmos a un problema en el álgebra lineal, lo cual será posible gracias al resultante de Sylvester.

En efecto, si dos γ_k son iguales, es posible utilizar la suma de logaritmos para combinar dos logaritmos en uno. Entonces, únicamente es necesario considerar aquellos γ_k que no sean iguales entre sí. Dado que b es libre de cuadrados, entonces no tiene raíces múltiples, y todas sus raíces serán polos de orden 1 para a/b por la propiedad 5.7. Sea β una raíz arbitraria de b. Entonces, representando a/b a través de su serie de Laurent centrada en β (teorema 5.3), esto implica que

$$\frac{a}{b} = \frac{\gamma}{x-\beta} + \sum_{k=0}^{\infty} c_k (x-\beta)^k. \tag{8.8}$$

Esto es importante, pues al integrar esta expresión se obtiene:

$$\int \frac{a}{b} = \gamma \log(x-\beta) + \sum_{k=0}^{\infty} \frac{c_k}{k+1}(x-\beta)^{k+1}.$$

Este hecho sugiere que cada γ_k no es más que el residuo de a/b en su polo β_k. Como este polo es de orden 1, su cálculo se resume nada más aplicar el teorema 5.4 para $m = 1$:

$$\gamma = \lim_{z\to\beta}(z-\beta)\frac{a(z)}{b(z)} = \lim_{z\to\beta}\frac{a(z)}{b(z)/(z-\beta)} = \frac{a(\beta)}{\lim_{z\to\beta} b(z)/(z-\beta)}.$$

Pero dado que $b(\beta) = 0$, se sigue que

$$\lim_{z\to\beta}\frac{b(z)}{z-\beta} = \lim_{z\to\beta}\frac{b(z)-b(\beta)}{z-\beta} = b'(\beta).$$

Por lo tanto, se llega a la siguiente expresión general para calcular el residuo de a/b en cada polo de orden 1 que posee:

$$\gamma = \frac{a(\beta)}{b'(\beta)}, \qquad \text{o} \qquad a(\beta) - \gamma b'(\beta) = 0. \tag{8.9}$$

De esta manera, es claro que para encontrar los coeficientes γ_k en frente de cada logaritmo se puede traducir a encontrar los ceros del polinomio

$$\prod_{\beta \mid b(\beta)=0} (a(\beta) - zb'(\beta)) \in K_b[z]. \tag{8.10}$$

El teorema 5.2 hace referencia a productos de este tipo, y es a través de dicho teorema que afirmamos que $\prod_{\beta|b(\beta)=0}(a(\beta) - zb'(\beta))$ es un múltiplo constante del polinomio $\mathrm{res}_x(a(x) - zb'(x), b(x))$ sobre la variable z. Con esto, ambas funciones presentan exactamente los mismos ceros. Pero puesto que $a(x)$ y $b(x)$ son polinomios sobre K, debe darse que el resultante se encuentra en $K[z]$, evitando así el uso del campo de descomposición K_b. Así, es posible reducir el problema a encontrar los ceros de

$$R(z) = \mathrm{res}_x(a(x) - zb'(x), b(x)) \in K[z]. \tag{8.11}$$

En consecuencia, cuando R posea raíces repetidas, se podrá reducir la cantidad de términos logarítmicos requeridos. Luego, se podrá expresar la integral como

$$\int \frac{a}{b} = \sum_{k=1}^{n} c_k \log(v_k), \tag{8.12}$$

donde $n \leq \deg(b)$, cada c_k es una raíz distinta de $R(z)$, y los v_k son polinomios mónicos, libres de cuadrados, y relativamente primos por pares, al ser productos de los $x - \beta_k$ para β_k distintos.

Esta discusión presenta la intuición detrás de presentar al resultante $R(z)$, pero no demuestra formalmente lo afirmado en la ecuación 8.12. Dicho problema se resuelve a continuación, y la necesidad de usar todas las raíces distintas de $R(z)$ para expresar la integral, así como un mecanismo para calcular los c_k y v_k mencionados, se demuestran en el teorema a continuación.

Teorema 8.3 (Segundo teorema de Rothstein-Trager para funciones racionales)**:** Sea $K(x)$ un campo diferencial en el cual $K = \operatorname{con}(K(x))$. Sea $a/b \in K(x)$ tal que $(a, b) = 1$, con b mónico, libre de cuadrados, y $\deg(a) < \deg(b)$. Supóngase que $\int a/b$ puede ser expresada como en la ecuación 8.12, donde $c_j \in K$ son distintos de cero y $v_j \in K[x]$ son mónicos, libres de cuadrados, no constantes, y $(v_i, v_j) = 1$ para cada $v_i \neq v_j$. Entonces, los c_j son las n raíces distintas del polinomio $R(z) = \operatorname{res}_x(a(x) - zb'(x), b(x)) \in K[z]$, y cada v_j está dado por $v_j = (a - c_j b', b) \in K[x]$.

Demostración. Dado el supuesto de la ecuación 8.12, es posible diferenciar ambos lados de la misma para llegar a la expresión

$$\frac{a}{b} = \sum_{k=1}^{n} c_k \frac{v_k'}{v_k}. \tag{8.13}$$

Ahora bien, si se multiplicara el lado izquierdo por b y el lado derecho por todos los posibles v_k, se eliminarían las fracciones y sería posible trabajar exclusivamente con polinomios. De hecho, podría plantearse la hipótesis de que $b = \prod_{k=1}^{n} v_k$. Esto se demostrará a continuación. Escríbase para cada índice j la expresión

$$u_j = \prod_{\substack{1 \le k \le n \\ k \neq j}} v_k.$$

Desde luego, esto implica que $\prod_{k=1}^{n} v_k = u_j v_j$. Multiplicando la ecuación 8.13 por $b \prod_{k=1}^{n} v_k$, que equivale a $b u_j v_j$ para cualquier $1 \le j \le n$, se obtiene

$$a \prod_{k=1}^{n} v_k = b \sum_{k=1}^{n} c_k v_k' u_k. \tag{8.14}$$

Esto implica que $b \mid \prod_{k=1}^{n} v_k$, gracias a que $(a, b) = 1$. Ahora, de la ecuación 8.14, se sigue para todo j que $v_j \mid b \sum_{k=1}^{n} c_k v_k' u_k$. Además, por la forma de los u_k, se sabe que $v_j \mid u_k$ para todo k distinto de j. Por tanto, v_j divide a cada sumando, y entonces es necesario que $v_j \mid b v_j' u_j$. Como v_j es libre de cuadrados, se tiene $(v_j, v_j') = 1$; y como $(v_i, v_j) = 1$ para cada $v_i \neq v_j$, dada la forma de los u_j también se tendrá que $(u_j, v_j) = 1$. Juntando estos hechos, es necesario que $v_j \mid b$ para todo j. Entonces, $\prod_{k=1}^{n} v_k \mid b$. Por doble divisibilidad, y al ser mónicos, esto implica la igualdad deseada:

$$b = \prod_{k=1}^{n} v_k. \tag{8.15}$$

Por tanto, la ecuación 8.14 puede reescribirse como

$$a = \sum_{k=1}^{n} c_k v_k' u_k. \tag{8.16}$$

Estas últimas dos ecuaciones nos ayudarán a demostrar que $v_j = (a - c_j b', b)$, como se requiere.

Primero, nótese de 8.15 que $b' = \sum_{k=1}^{n} v_k' u_k$ por la regla del producto. Entonces, combinando esto con la ecuación 8.16,

$$a - c_j b' = \sum_{k=1}^{n} c_k v_k' u_k - c_j \sum_{k=1}^{n} v_k' u_k = \sum_{k=1}^{n} (c_k - c_j) v_k' u_k. \tag{8.17}$$

De nuevo, cuando $k \neq j$, se sabe que $v_k \mid u_k$. Si $k = j$, entonces $c_k - c_j = 0$. Por lo tanto, v_j divide a cada término de la suma en 8.17, y por lo tanto $v_j \mid a - c_j b'$. Además, también es claro de 8.15 que $v_j \mid b$. Simplemente queda demostrar que v_j es máximo en esta relación de divisibilidad: si existe otro polinomio que divida a $a - c_j b'$ y a b, entonces también divide a v_j. Pero nótese que, como se demostró la divisibilidad de ambos por v_j, se desea calcular

$$(a - c_j b', b) = \left(v_j \cdot \frac{a - c_j b'}{v_j}, v_j \prod_{\substack{1 \le k \le n \\ k \neq j}} v_k \right) = v_j \left(\frac{a - c_j b'}{v_j}, \prod_{\substack{1 \le k \le n \\ k \neq j}} v_k \right).$$

Pero si se tuviera que $(a - c_j b', v_i) = 1$ para todo $i \neq j$, sería claro que $\left(\frac{a-c_jb'}{v_j}, \prod_{k\neq j}^{1\leq k\leq n} v_k\right) = 1$ y el resultado se seguiría inmediatamente. En efecto, esto es lo que se demostrará a continuación. Considérese v_i para un $i \neq j$. Entonces, dado que $v_i \mid u_k$ para todo $i \neq k$, entonces

$$(a - c_j b', v_i) = \left(\sum_{k=1}^{n}(c_k - c_j)v_k' u_k, v_i\right) = \big((c_i - c_j)v_i' u_i, v_i\big).$$

Pero como $i \neq j$, entonces $c_i - c_j \neq 0$, y se tiene que $(v_i, v_i') = 1$ por ser v_i libre de cuadrados, y $(v_i, u_i) = 1$. Con esto, $\big((c_i - c_j)v_i' u_i, v_i\big) = 1$, por lo cual en efecto $(a - c_j b', v_i) = 1$, y por lo tanto

$$v_j = (a - c_j b', b). \tag{8.18}$$

Considérese ahora al polinomio $R(z) = \mathrm{res}_x(a(x) - zb'(x), b(x))$. Siendo este un resultante, y dado que $v_j = (a - c_j b', b)$ es no constante según la hipótesis dada, se debe tener por el criterio de Sylvester 5.5 que $R(c_j) = \mathrm{res}_x(a(x) - c_j b'(x), b(x)) = 0$. Esto es, cada c_j es un cero de R.

Ahora, supóngase que existe otro posible cero c de R en su campo de descomposición. Entonces de nuevo por el criterio de Sylvester se asegura que $t = (a - cb', b)$ es un polinomio no constante. Tomemos un factor irreducible s de t. Por transitividad se tiene que $s \mid b$ y que $s \mid (a - cb')$, y como los v_k son primos relativos por pares, la primera de estas implica que existe un único v_k divisible por s. En cuanto a la segunda, se tiene que $s \mid \sum_{k=1}^{n}(c_k - c)v_k' u_k$ por la relación 8.17. Pero dado que $s \mid v_j$ para un solo j, entonces $s \mid u_k$ para cada $k \neq j$. Desde luego, esto implica que $s \mid (c_j - c)v_j' u_j$.

Ahora bien, nótese que $s \nmid u_j$ puesto que este es el producto de todos los v_k distintos de v_j, los cuales son primos relativos por pares; y también obsérvese que $s \nmid v_j'$, pues se tiene que $s \mid v_j$ y que $(v_j, v_j') = 1$ por la cualidad de polinomio libre de cuadrados de v_j. Finalmente, se concluye que la única forma de que $s \mid (c_j - c)v_j' u_j$ es que esta expresión se anule, lo cual solo ocurre si $c = c_j$ para el índice j en el cual $s \mid v_j$. Esto demuestra que R se descompone por completo sobre K, y que los c_j propuestos son todas sus raíces.

■

Esto provee un mecanismo completamente general para calcular la antiderivada de cualquier función racional. A continuación, se muestra un ejemplo.

Ejemplo 8.2: Considérese la integral $\int \frac{x^3-1}{x^2-4}\,\mathrm{d}x$. Utilizando el algoritmo de la división, se llega enseguida a

$$\int \frac{x^3 - 1}{x^2 - 4}\,\mathrm{d}x = \frac{x^2}{2} + \int \frac{4x - 1}{x^2 - 4}.$$

Para la integral restante, es posible utilizar el teorema 8.3. Se tiene $a(x) = 4x - 1$ y $b(x) = x^2 - 4$, con lo cual $b'(x) = 2x$. Así,

$$\begin{aligned} R(z) = \mathrm{res}_x(a(x) - zb'(x), b(x)) &= \mathrm{res}_x((4 - 2z)x - 1, x^2 - 4) \\ &= \det\left(\begin{bmatrix} 4-2z & -1 & 0 \\ 0 & 4-2z & -1 \\ 1 & 0 & -4 \end{bmatrix}\right) = 1 - 4(4 - 2z)^2. \end{aligned}$$

De esta manera, se obtiene que los ceros de $R(z)$ son $c_1 = 9/4$ y $c_2 = 7/4$. Con esto, es posible calcular $v_1(x)$ y $v_2(x)$:

$$\begin{aligned} v_1(x) &= \left(a(x) - \frac{9}{4}b'(x), x^2 - 4\right) = (x + 2, x^2 - 4) = x - 2, \\ v_2(x) &= \left(a(x) - \frac{7}{4}b'(x), x^2 - 4\right) = (x - 2, x^2 - 4) = x + 2. \end{aligned}$$

Como nota, en el cálculo de los máximos comunes divisores se utilizó la unicidad del mismo salvo asociación. Finalmente, juntamos los resultados obtenidos y se tiene que

$$\int \frac{x^3-1}{x^2-4}\,\mathrm{d}x = \frac{x^2}{2} + \frac{9}{4}\log(x+2) + \frac{7}{4}\log(x-2).$$

Para finalizar con los teoremas de Rothstein-Trager para funciones racionales, se demuestra a continuación que el campo de constantes generado por su algoritmo es mínimo.

Teorema 8.4 (Tercer teorema de Rothstein-Trager para funciones racionales)**:** Sea $K(x)$ un campo diferencial tal que $K = \mathrm{con}(K(x))$. Sea $a/b \in K(x)$ tal que $(a,b) = 1$, con b mónico, libre de cuadrados, y $\deg(a) < \deg(b)$. Sea K^* la extensión algebraica más pequeña de K tal que existan $c_k^* \in K^*$ y $v_k^* \in K^*[x]$ para los cuales sea posible escribir

$$\int \frac{a}{b} = \sum_{k=1}^{n^*} c_k^* \log(v_k^*).$$

Entonces, debe darse que $K^* = K(c_1, c_2, \cdots, c_n)$, donde c_k son las n raíces distintas del polinomio $R(z) = \mathrm{res}_x(a(x) - zb'(x), b(x)) \in K[z]$. Es decir, K^* es el campo de descomposición de $R(z) \in K[z]$.

Demostración. Supóngase que es posible escribir la integral como se mostró con los $c_k^* \in K^*$ y $v_k^* \in K^*[x]$ respectivos. Nótese que, según los supuestos, estos no necesariamente cumplirán los requerimientos del segundo teorema de Rothstein-Trager. En caso de no cumplirse dicho requerimiento para un v_k^*, escríbase la factorización libre de cuadrados del mismo como $v_j^* = \prod_{k=1}^{n} v_k^k$, donde cada v_k es libre de cuadrados, y $(v_i, v_j) = 1$ para $i \neq j$. Usando las propiedades 7.1 y 7.2 de los logaritmos,

$$\log\bigl(v_j^*\bigr) = \log\left(\prod_{k=1}^{n} v_k^k\right) = \sum_{k=1}^{n} k \log(v_k).$$

Si algún v_k no es mónico en esta instancia, es posible volverlo mónico factorizando su coeficiente principal y usando de nuevo la propiedad de suma de logaritmos. Esto únicamente provoca una suma por una constante, lo cual entra en la clase de equivalencia de la antiderivada. De esta manera, sin pérdida de la generalidad, es posible asumir que los v_k^* dados por la hipótesis son polinomios mónicos libres de cuadrados.

Ahora bien, supóngase que $(v_i^*, v_j^*) = v$ para un polinomio $v \in K^*[x]$ no constante, y para $v_i^* \neq v_j^*$. Luego, de nuevo gracias a las propiedades del logaritmo,

$$\log\bigl(v_j^*\bigr) = \log\bigl(v \cdot v_j^*/v\bigr) = \log(v) + \log\bigl(v_j^*/v\bigr),$$

y lo mismo para v_i^*. Pero aquí, es claro que v y v_j^*/v son polinomios dentro de $K^*[x]$, y que ambos son mónicos y libres de cuadrados. Este proceso puede realizarse hasta lograr que todos los términos dentro de los logaritmos tengan máximo común divisor 1, y juntando aquellos que tengan el mismo argumento. Ahora, si se tiene $c_i^* = c_j^*$ para algún $i \neq j$, se escribe entonces

$$c_i^* \log(v_i^*) + c_j^* \log\bigl(v_j^*\bigr) = c_i^* \log\bigl(v_i^* \cdot v_j^*\bigr).$$

De nuevo, esto nos lleva a un argumento del logaritmo donde $v_i^* \cdot v_j^*$ será mónico, libre de cuadrados, y primo relativo de cualquier otro argumento. Esto es, la expresión dada para la integral es en efecto equivalente a la expresión que se necesita para la hipótesis del segundo teorema de Rothstein-Trager. Finalmente, usando dicho teorema, se llega a que los c_k^* son raíces de $R(z) = \mathrm{res}_x(a(x) - zb'(x), b(x))$, y los v_k^* pueden escribirse con $v_k^* = (a - c_k^* b', b)$. Desde luego, esto implica que K^* es, en efecto, el campo de descomposición de $R(z)$.

■

Aunque este algoritmo ya es una mejora con respecto al uso exhaustivo de fracciones parciales, es posible mejorar aún más el tiempo de corrida del algoritmo de Rothstein-Trager a través de subresultantes de Sylvester. Dicha mejora es conocida por el nombre de Lazard-Rioboo-Trager, y puede conocerse más al respecto en el artículo de Lazard y Rioboo [14]. En este trabajo, el algoritmo original será suficiente para cumplir con los objetivos requeridos. A continuación, se muestra el algoritmo que nace de los teoremas de Rothstein-Trager.

Algoritmo 8.2: Algoritmo de Rothstein-Trager.

1. Tomar una función racional $a/b \in K(x)$, como la que resulta de la parte logarítmica del algoritmo de Hermite: con b monico, libre de cuadrados, y con $\deg(a) < \deg(b)$.
2. Se calcula el polinomio $R(z) = \text{res}_x\left(a(x) - zb'(x), b(x)\right)$.
3. Se factoriza el polinomio $R(z)$ en n factores $R_1(z), R_2(z), \ldots, R_n(z)$.
4. Inicializar la integral como $I = 0$.
5. Se inicia un contador en $k = 1$ que llegará hasta n.
   - Se escribe $d = \deg(R_k(z))$.
   - Si $d = 1$, entonces se realiza lo siguiente:
     - Se escribe que c es el despeje lineal de la variable z en la ecuación $R_k(z) = 0$.
     - Se escribe $v = (a - cb', b)$.
     - Se reemplaza v por él mismo dividido entre su coeficiente principal.
     - Se reemplaza I por $I + c\log(v)$.
   - Si $d \neq 1$, entonces se realiza lo siguiente:
     - Se escribe $v = (a - \alpha b', b)$, donde α es una raíz de $R_k(z)$.
     - Se reemplaza v por él mismo dividido entre su coeficiente principal.
     - Escribir c_j para $1 \leq j \leq d$ como las raíces de $R_k(z)$, calculando a través de métodos exactos cuando sea posible, o con métodos numéricos en el peor caso.
     - Se inicia un contador en $j = 1$ y termina en $j = d$.
       - Se escribe v_j como v sustituyendo α por c_j.
       - Se reemplaza I por $I + c_j \log(v_j)$.
       - Cuando se tenga en I una suma con $c_i = c_j$ para $i \neq j$, se juntan los logaritmos.
6. Se devuelve al usuario el resultado de la integral logarítmica como I.

Principalmente, la existencia de los algoritmos 8.1 y 8.2 implica que la integral de toda función racional en $K(x)$ existe y puede ser expresada usando una cantidad finita de logaritmos con argumentos polinomiales. Es decir, la solución vive en $K(c_1, c_2, \ldots, c_n)(x, \log(v_1), \log(v_2), \ldots, \log(v_n))$. Así, observamos que la antiderivada de un elemento de $K(x)$ siempre es elemental, y podrá expresarse a través de un elemento de $K(x)$ y de logaritmos cuya entrada sea un elemento de $K(x)$. El siguiente capítulo trabajará sobre esta observación, y buscará generalizarla para obtener un criterio que determine la forma que debe tener la antiderivada de una función elemental.

CAPÍTULO 9

Principio de integración de Liouville

El capítulo anterior se concentró en demostrar que una función racional en $K(x)$, donde K es un campo de característica 0, siempre posee una antiderivada elemental. De hecho, logró demostrarse que para ello no es necesario más que una cantidad finita de extensiones logarítmicas y de constantes en el campo. El resultado cumbre en la teoría de integración de funciones elementales es debido a Liouville, y es una generalización del comportamiento visto en las funciones racionales.

9.1. El sistema de casos simples de Liouville

El principio de Liouville enunciado de manera intuitiva afirma lo siguiente: para que sea elemental la antiderivada de una función que se encuentra en un campo diferencial F, es necesario que esta pueda escribirse como una función perteneciente a F, sumada a logaritmos de funciones que también se encuentran en F. En otras palabras, el único tipo *nuevo* de función que puede aparecer en la expansión de una antiderivada elemental es un logaritmo, de manera que las funciones exponenciales y algebraicas solo aparecen si se encuentran en el campo diferencial original F. En efecto, este es un comportamiento más general de lo que se observó en el caso de las funciones racionales. Sin embargo, ahora es necesario demostrarlo para campos diferenciales generales y arbitrarios, por lo cual la herramienta utilizada en el capítulo 8 no se encuentra disponible.

Una estrategia para demostrar un teorema complejo consiste en separar la solución en distintas partes. En nuestro caso, ocurre que el comportamiento de las funciones elementales difiere mucho dependiendo de si son exponenciales, logarítmicas o algebraicas. Es por ello que será necesario demostrar primero tres casos especiales, cada uno de ellos correspondiendo a los tres tipos de funciones elementales simples. Para las logarítmicas, mostraremos que estas pueden aparecer en la antiderivada. Para las exponenciales y algebraicas, demostraremos que no. Y para cada uno de ellos, será importante utilizar su teorema de diferenciación correspondiente, pues estos dan una forma muy rígida a las derivadas y antiderivadas de las funciones elementales. Luego, se buscará usar un argumento inductivo sobre la cantidad de extensiones necesarias para encontrar el campo diferencial de extensión sobre el cual se presenta la antiderivada de la función dada. Pero primero, enunciamos y demostramos el teorema en sus casos simples.

El caso más natural, como se observará en lo que resta de esta teoría, es el caso logarítmico. Por ello, es el primero en demostrarse.

Teorema 9.1 (Principio de Liouville para extensiones logarítmicas simples)**:** Sea F un campo diferencial, y sea $f \in F$. Supóngase que $\int f$ se encuentra en la extensión trascendental elemental $G = F(g)$, donde $g = \log(v_1)$ para una función $v_1 \in F$, y que además $\operatorname{con}(F) = \operatorname{con}(G) = K$. Entonces, existen $v_0 \in F$ y $c_1 \in K$ tales que

$$\int f = v_0 + c_1 \log(v_1).$$

Demostración. Sea $F = K(x, g_1, g_2, \ldots, g_n)$ el campo diferencial a trabajar, donde $K = \operatorname{con}(F)$. Además, supóngase que $\int f \in G$, donde $G = F(g)$ para un logaritmo trascendental $g = \log(v_1)$ con $v_1 \in F$. De esta manera, existen polinomios $a, b \in F[g]$ tales que $(a, b) = 1$ y b sea mónico tales que

$$\int f = \frac{a(g)}{b(g)}.$$

Ahora, como se vio en la prueba del algoritmo de Hermite en el capítulo 8, es posible factorizar $b(g)$ en sus factores libres de cuadrados con $b(g) = \prod_{k=1}^{m} b_k(g)^{\alpha_k}$. Realizando el algoritmo de la división y luego fracciones parciales para $a(g)/b(g)$ sobre $F[g]$, esto es

$$\int f = \frac{a(g)}{b(g)} = a_0(g) + \sum_{k=1}^{m} \sum_{j=1}^{\alpha_k} \frac{a_{kj}(g)}{b_k(g)^j}.$$

En esta expresión, $a_0, a_{kj}, b_k \in F[g]$ para $1 \leq k \leq m$, y $\deg(a_{kj}) < \deg(b_k)$. Diferenciando esta expresión por ambos lados,

$$f = [a_0(g)]' + \sum_{k=1}^{m} \sum_{j=1}^{\alpha_k} \left(\frac{b_k(g)^j [a_{kj}(g)]' - j b_k(g)^{j-1} [b_k(g)]' a_{kj}(g)}{b_k(g)^{2j}} \right)$$

Y simplificando la expresión en la sumatoria, esto es

$$f = [a_0(g)]' + \sum_{k=1}^{m} \sum_{j=1}^{\alpha_k} \left(\frac{[a_{kj}(g)]'}{b_k(g)^j} - \frac{j a_{kj}(g) [b_k(g)]'}{b_k(g)^{j+1}} \right). \tag{9.1}$$

Nótese que, como $f \in F$ es independiente de g, entonces el lado derecho también lo es. Supóngase así que la doble suma en la derecha de la ecuación es no nula e independiente de g. Considérese uno de los $b_k(g)$ irreducibles y mónicos con $\deg(b_k(g)) > 0$. Este es un polinomio con entradas logarítmicas, y cumpliéndose los primeros dos puntos del teorema 7.2, entonces en primera $[b_k(g)]' \in F[g]$, y en segunda $\deg([b(g)]') = \deg(b(g)) - 1$. Desde luego, es claro entonces que $b_k(g) \nmid [b_k(g)]'$. Además, no existen polinomios en $F[g]$ que dividan a $b_k(g)$ por ser irreducible. Así, en la ecuación 9.1, el término con denominador $b_k(g)^{\alpha_k+1}$ permanece sin poderse simplificar. Al no existir otro término con el cual pudiera cancelarse, entonces este aparece en la expansión de f, haciendo que esta dependa de g. Esto es imposible, de manera que

$$f = [a_0(g)]',$$

donde $a_0 \in F[g]$ y $[a_0(g)]'$ no depende de g, que por el teorema 7.2 solo ocurre si existe una constante $c_1 \in K$ y una función $v_0 \in F$ tales que $a_0(g) = v_0 + c_1 g$. Como $g = \log(v_1)$, entonces

$$\int f = v_0 + c_1 \log(v_1).$$

■

El anterior teorema demuestra que, si f pertenece a un campo diferencial F, entonces un nuevo logaritmo cuya entrada es una función en F puede aparecer en la expansión de $\int f$. Esto va acorde a lo que se ha discutido, y es lo que se observó en el algoritmo de Rothstein-Trager. Lo que se busca ahora es demostrar que lo mismo no ocurre para las funciones exponenciales o algebraicas, mostrando la imposibilidad de obtener funciones exponenciales o algebraicas nuevas a la hora de integrar una función.

Teorema 9.2 (Principio de Liouville para extensiones exponenciales simples)**:** Sea F un campo diferencial, y sea $f \in F$. Supóngase que $\int f$ se encuentra en la extensión trascendental elemental $G = F(g)$, donde $g = \exp(v_1)$ para una función $v_1 \in F$, y que además $\operatorname{con}(F) = \operatorname{con}(G) = K$. Entonces,

$$\int f \in F.$$

Demostración. Para la demostración del teorema 9.1 únicamente se utilizó que g es una función trascendental sobre F. Por lo tanto, todo lo realizado hasta la ecuación 9.1 aplica en el presente caso, de manera que también se tiene

$$f = [a_0(g)]' + \sum_{k=1}^{m} \sum_{j=1}^{\alpha_k} \left(\frac{[a_{kj}(g)]'}{b_k(g)^j} - \frac{j a_{kj}(g)[b_k(g)]'}{b_k(g)^{j+1}} \right).$$

De nuevo, $f \in F$ es independiente de g, por lo cual el lado derecho también debe serlo. Considérese de nuevo a uno de los $b_k(g)$ irreducibles y mónicos con $\deg(b_k(g)) > 0$. Este es un polinomio con entradas exponenciales y coeficiente principial 1. Supóngase primero que $b_k(g)$ no es un monomio. Entonces, por la tercera parte del teorema 7.3, se tiene $b_k(g) \nmid [b_k(g)]'$. Los argumentos utilizados en este caso para el teorema 9.1 aplican, y se llegaría a la misma contradicción. Por lo tanto, $b_k(g)$ es un monomio. Pero al ser mónico e irreducible en $F[g]$, solo puede ser que $b_k(g) = g$. Además, recordando que $b(g) = \prod_{k=1}^{m} b_k(g)^{\alpha_k}$ y haciendo $\alpha = \sum_{k=1}^{m} \alpha_k$, se tiene

$$\int f = \frac{a(g)}{b(g)} = \frac{a(g)}{g^\alpha} = \sum_{k=-\alpha}^{\deg(a(g))-\alpha} v_k g^k,$$

para $v_k \in F$. Diferenciando y utilizando la primera parte del teorema 7.3, entonces afirmamos que para cada $v_k \neq 0$ existen $\bar{v_k} \in F$ no nulos tales que

$$f = v_0' + \sum_{k \neq 0}^{-\alpha \leq k \leq \deg(a(g))-\alpha} \bar{v_k} g^k,$$

omitiendo el caso de $k = 0$ como dicho teorema explicita. Sin embargo, siendo f independiente de g, debería darse $\bar{v_k} = 0$ para cada $k \neq 0$, lo cual solo puede ocurrir si $v_k = 0$ para dichos índices. En cualquier caso, se da entonces que $f = v_0'$, de lo cual

$$\int f = v_0 \in F.$$

■

La importancia de este caso del teorema de Liouville radica en observar que esto implica la imposibilidad de encontrar una nueva extensión exponencial en la solución simbólica de la integral. Es decir, únicamente puede aparecer una función exponencial si esta ya pertenecía al campo diferencial del cual es parte el integrando. A continuación, debemos demostrar un resultado similar para las extensiones algebraicas, concluyendo con los casos simples del principio de Liouville.

Teorema 9.3 (Principio de Liouville para extensiones algebraicas simples)**:** Sea F un campo diferencial, y sea $f \in F$. Supóngase que $\int f$ se encuentra en la extensión algebraica elemental $G = F(g)$, donde g es algebraico sobre F, y que además $\text{con}(F) = \text{con}(G) = K$. Entonces,

$$\int f \in F.$$

Demostración. Sea $p(z) \in F[z]$ el polinomio mínimo que satisface a g, de modo que $p(g) = 0$, y escríbase $\deg(p(z)) = N + 1$. Escríbase $\int f = a(g) \in F(g)$. Entonces, $f = [a(g)]'$. Escríbanse las $N + 1$ raíces de $p(z)$ como $g_0, g_1, \ldots, g_N$. Como f es independiente de f, y debido a la unicidad del operador diferencial como visto en la propiedad 7.5, entonces $f = [a(g_k)]'$ para todo subíndice k entre 0 y N. Entonces,

$$f = \frac{1}{N+1} \sum_{k=0}^{N} [a(g_k)]'.$$

Esto puede reescribirse $f = v_0'$, donde

$$v_0 = \frac{1}{N+1} \sum_{k=0}^{N} a(g_k).$$

Aquí, v_0 es una función simétrica en $F(g_0, g_1, \ldots, g_N)$, e invariante bajo permutaciones de los g_k. El teorema fundamental de las funciones simétricas (véase el capítulo 5.6 de [12]) implica que toda función simétrica en los símbolos $g_0, g_1, \ldots, g_N$ puede ser completamente expresada en términos de su polinomio mínimo en F. Esto es, dicha función está completamente determinada por elementos de F. Por lo tanto,

$$\int f = v_0 \in F.$$

■

Como en el caso exponencial, esto demuestra que la integral de una función nunca requiere de nuevas extensiones algebraicas en su solución simbólica.

9.2. El principio general de Liouville

Se ha demostrado el teorema de Liouville para una sola extensión elemental de cualquier tipo. Sin embargo, el resultado general incluye una cantidad finita de extensiones sobre el campo diferencial original. Esto nos lleva a un argumento inductivo, como se discutió con anterioridad. Seguidamente, se presenta el principio general de Liouville, utilizando dicho argumento inductivo.

Teorema 9.4 (Principio de Liouville)**:** Sea F un campo diferencial. Para $f \in F$, supóngase que $\int f$ se encuentra en G, una extensión elemental de F tal que $\text{con}(F) = \text{con}(G) = K$. Entonces, existen funciones $v_0, v_1, v_2, \ldots, v_m \in F$ y constantes $c_1, c_2, \ldots, c_m \in K$ tales que

$$\int f = v_0 + \sum_{k=1}^{m} c_k \log(v_k). \tag{9.2}$$

A través de la ecuación 9.2, es mucho más aparente que el principio de Liouville es un caso general de lo que ocurrió en las funciones racionales. Para su demostración, será necesario utilizar los casos especiales demostrados a lo largo de este capítulo.

Demostración. Supóngase que existen $g_1, g_2, \ldots, g_N$ tales que $G = F(g_1, g_2, \ldots, g_N)$, donde cada g_k sea logarítmica, exponencial, o algebraica sobre $F_{k-1} = F(g_1, g_2, \ldots, g_{k-1})$, que además cada F_k posee el mismo campo de constantes K, y que existe $\gamma \in G$ tal que $\gamma = \int f$. Se procede por inducción sobre N, la cantidad de extensiones elementales de F que aparecen en G necesarias para cumplir la ecuación 9.2. El caso base es $N = 0$, donde $F_0 = G$, de manera que $\gamma \in G$, y se cumple la ecuación 9.2 tomando $v_0 = \gamma$, y $c_k = 0$ para cada índice k. También se cumple el caso $N = 1$ gracias a los casos simples demostrados con anterioridad. Tomemos como hipótesis inductiva, entonces, que el teorema de Liouville se cumple para cualquier número de extensiones menor a N.

Considérese entonces el caso de N extensiones. Como $f \in F$, entonces también $f \in F(g_1)$, mientras que $\gamma \in F(g_1)(g_2, \ldots, g_N)$ es tal que $\gamma = \int f$. Escríbase $g = g_1$. Entonces, aplicando la hipótesis inductiva, existen funciones $v_k(g) \in F(g)$ y constantes $c_k \in K$ para índices $1 \leq k \leq m$ tales que

$$f = [v_0(g)]' + \sum_{k=1}^{m} c_k \frac{[v_k(g)]'}{v_k(g)}. \tag{9.3}$$

Existen tres casos, siendo estos que g puede ser trascendental logarítmica o exponencial, o bien algebraica. Supóngase primero que g es logarítmica trascendental sobre F. Por argumentos similares a los de los teoremas de Rothstein-Trager, podemos asumir sin perder generalidad que cada $v_k(g)$ es elemento de F, o bien, mónico e irreducible en $F[g]$ con $\deg(v_k(g)) > 0$. Además, que cada $v_i(g) = v_j(g)$ si y solo si $i = j$, y que los c_k son no nulos. Ahora, escríbase $v_0(g) = a(g)/b(g)$ para $a, b \in F[g]$, donde $(a, b) = 1$ y b es mónico. De nuevo, es posible expresar $v_0(g)$ de la manera siguiente usando el algoritmo de la división y fracciones parciales:

$$v_0(g) = a_0(g) + \sum_{k=1}^{m} \sum_{j=1}^{\alpha_k} \frac{a_{kj}(g)}{b_k(g)^j},$$

donde $a_0, a_{kj}, b_j \in F[g]$, y $\deg(a_{kj}) < \deg(b_j)$. De esta manera, diferenciando, las ecuaciones 9.2 y 9.3 se amalgaman de manera que

$$f = [a_0(g)]' + \sum_{k=1}^{m} \sum_{j=1}^{\alpha_k} \left(\frac{[a_{kj}(g)]'}{b_k(g)^j} - \frac{j a_{kj}(g)[b_k(g)]'}{b_k(g)^{j+1}} \right) + \sum_{k=1}^{m} c_k \frac{[v_k(g)]'}{v_k(g)}. \tag{9.4}$$

Como en las pruebas anteriores, es importante notar que f no depende de g, por lo cual el lado derecho debe deshacerse de su dependencia de g de alguna manera.

Dado que g es logarítmica sobre F, existe $u \in F$ tal que $g' = u'/u$. Defínase $p(g) \in F[g]$ como un polinomio irreducible y mónico con $\deg(p) > 0$. Entonces, por el teorema 7.2, se tiene $[p(g)]' \in F[g]$ con $\deg([p(g)]') = \deg(p(g)) - 1$, de manera que $p(g) \nmid [p(g)]'$. Supóngase que $p(g) = b_k(g)$, de forma que aparezca en la expansión de la ecuación 9.4 con potencia α_k. Entonces, el lado derecho de la ecuación contiene un solo término con denominador $p(g)^{\alpha_k+1}$, donde $\alpha_k > 0$. Dado que este término no posee ningún otro con cual cancelarse en la expansión, debería aparecer en el lado izquierdo de la ecuación. Pero este depende de g, por lo cual sería absurdo que apareciera en f. De esta manera, la doble sumatoria en la ecuación debe anularse por completo. Si por otro lado se supone que $p(g) = v_k(g)$, entonces existe un término con denominador dependiente de g que no puede anularse, por lo cual de nuevo se llega al mismo absurdo. Entonces, debe ocurrir que los $v_k(g)$ no pertenezcan a $F[g]$, pero sí a F, por lo que los reescribimos como $v_k \in F$. Luego,

$$f = [a_0(g)]' + \sum_{k=1}^{m} c_k \frac{v_k'}{v_k}.$$

Finalmente, $[a_0(g)]'$ debe ser independiente de g, lo cual solo puede ocurrir cuando $a_0(g) = c_0 g + u_0$, para $c_0 \in K$ y $u_0 \in F$. Así, como se requeriría en el enunciado de Liouville,

$$f = u_0' + c_0 \frac{u'}{u} + \sum_{k=1}^{m} c_k \frac{v_k'}{v_k} \implies \int f = u_0 + c_0 \log(u) + \sum_{k=1}^{m} c_k \log(v_k).$$

Finalmente, supóngase que $g_1 = g$ es una extensión exponencial trascendental, o una extensión algebraica. Pero los teoremas 9.2 y 9.3 demuestran que esto resultaría inmediatamente en que $\int f$ permanecería en $F(g_2, \ldots, g_N)$, de manera que una nueva extensión exponencial o algebraica no es necesaria para expresar la integral.

■

Es claro que el principio de Liouville le da una gran importancia a los logaritmos, gracias a sus propiedades diferenciales. La aparición de las extensiones exponenciales y algebraicas es necesaria para apreciar cómo se ven restringidas estas funciones en cuanto a su aparición en una antiderivada simbólica, y debido a que son parte fundamental de las funciones elementales. Sin embargo, el estudio de la aparición de distintas funciones en la solución simbólica de una integral no se limita únicamente a las funciones elementales aquí observadas. Para evitar el uso de números complejos en el estudio de las antiderivadas, también es posible definir a las *funciones elementales reales*, para las cuales es necesario modificar ligeramente el principio de Liouville. Puede observarse un poco sobre estas funciones en el Anexo 14.2.

También resulta interesante considerar funciones no elementales, como lo son la integral exponencial, integral logarítmica, funciones de error, dilogaritmos, entre otras. También se definen algunas de dichas funciones en el Anexo 14.2 de este trabajo. Sin embargo, la presente investigación no tiene como propósito cubrir este tema, pero si se desea ahondar en resultados como estos puede visitarse el artículo de Baddoura [2]. Este posee definiciones para ciertos tipos de funciones no elementales, así como una versión extendida del principio de Liouville para las mismas. El logaritmo es especial en ser la única función elemental independiente que puede aparecer como una nueva función en la integración, siempre que se permita el uso de números complejos. Sin embargo, no es la única función nueva que puede surgir si no se restringe al uso de las funciones elementales, y es ahí donde se potencia el estudio de las funciones especiales.

Lo estudiado en este capítulo servirá como base para terminar con nuestro estudio de la integración elemental. Los resultados aquí demostrados permiten dar una forma general a la antiderivada de una función elemental, asumiendo que dicha antiderivada también resulta ser elemental. Esto provoca que, si se logra demostrar que una antiderivada no posee esta forma, entonces dicha antiderivada no puede ser una función elemental. Esta es la herramienta principal que será utilizada en las demostraciones del capítulo siguiente, y la que permite crear un algoritmo de integración de funciones elementales.

CAPÍTULO 10

Algoritmos de solución y decisión de Risch

La teoría desarrollada a lo largo de esta investigación tiene un doble propósito. El más alto interés se presenta en caracterizar o mostrar las condiciones necesarias para la existencia de antiderivadas elementales en una cantidad finita de términos. Sin embargo, también se tiene un interés muy fuerte por encontrar algoritmos de integración en caso que dicha antiderivada exista. En este capítulo se buscará abarcar ambos intereses, demostrando varios teoremas con las condiciones necesarias para la existencia de antiderivadas elementales, y desarrollando algoritmos que encuentren la solución en caso de existir. Estas tareas se complementan entre sí, por lo cual juntarlas se da naturalmente.

Discutiremos sobre la integración simbólica de funciones elementales en un campo diferencial $K(x, g_1, \ldots, g_N)$, donde $K \subseteq \mathbb{C}$ es el campo de constantes, cada g_k es elemental, y específicamente será trascendental, ya sea exponencial o logarítmica, sobre $F_{k-1} = K(x, g_1, \ldots, g_{k-1})$. Esto abarcará una gran cantidad de funciones, incluyendo la totalidad de las funciones trigonométricas e hiperbólicas habituales, y algunas cuantas de sus inversas. Para poder integrar también las funciones radicales, y funciones que las contengan como las inversas de algunas trigonométricas e hiperbólicas, es necesario ahondar en el caso de la integración de funciones elementales algebraicas, lo cual se daría cuando g_N sea algebraica sobre F_{N-1}. Este caso resulta ser bastante más complicado, al requerir herramientas de geometría algebraica computacional. Por ello, se deja fuera del alcance de esta tesis, pero puede consultarse en trabajos como el de Bronstein [4] y Trager [22]. La literatura correspondiente a este caso aún continúa expandiéndose, como puede observarse en artículos como el de Masser [17], siendo este un trabajo del año 2020.

Para resolver el problema de integración simbólica para un integrando elemental, se nos dará una función f a integrarse con respecto a un símbolo x, y primero se buscará determinar un campo diferencial F al cual la función f pertenezca. Este tendrá la forma mencionada anteriormente, donde $K = \mathrm{con}(F)$ es un subcampo de $\mathbb{C}$, y las funciones de extensión $g_k \in F$ serán trascendentales logarítmicas o exponenciales sobre los subcampos correspondientes F_{k-1}. Encontrar la forma más simple de estos campos no siempre es tan fácil, pero un entendimiento de la estructura e interacción de las funciones trascendentales debería ser suficiente para que una persona lo logre. Presentarle este problema a una computadora demuestra algunos retos adicionales, pero en nuestro caso no es necesario preocuparnos por ello. En general, se asumirá que un campo que cumpla esta descripción puede encontrarse exitosamente para continuar con los propósitos de este capítulo.

Ahora bien, dado que cada símbolo g_k es trascendental, entonces el integrando puede ser tratado como una función racional de estos símbolos en F. Es aquí donde radica la importancia de los algoritmos de integración de Hermite y Rothstein-Trager, pues serán utilizados para integrar funciones que son racionales en una variable g_k, en vez de sobre el símbolo habitual x. Esto, dado que $f \in K(x, g_1, \ldots, g_N)$ puede tratarse como una función racional

$$f(g_N) = \frac{p(g_N)}{q(g_N)} \in K(x, g_1, \ldots, g_{N-1})(g_N). \tag{10.1}$$

Como se ha hecho repetidas veces, esto puede hacerse asumiendo que $(p(g_N), q(g_N)) = 1$ y $q(g_N)$ es mónico, para $p(g_N), q(g_N) \in F_{N-1}[g_N]$. En cuanto a los símbolos a utilizarse para la diferenciación y antidiferenciación, se reserva el uso de f' y $\int f$ para derivadas y antiderivadas sobre x, mientras que $D_g[f]$ será utilizado cuando se desee diferenciar con respecto a otro símbolo g.

10.1. Extensiones logarítmicas trascendentales

A lo largo de esta sección, se tomará f como en la ecuación 10.1, donde g_N es una extensión logarítmica trascendental sobre F_{N-1}. Esto es, existe $u \in F_{N-1}$ tal que $g_N' = u'/u$, de manera que escribimos $g_N = \log(u)$.

El objetivo de las siguientes subsecciones será lograr integrar cualquier función elemental que pueda ser vista como un miembro de un campo de funciones elementales trascendentales cuya última extensión sea logarítmica. Para ello, se generalizarán los teoremas de integración de funciones racionales vistos en el capítulo 8, de manera que apliquen en el campo de funciones racionales sobre la variable g_N con coeficientes en $K(x, g_1, \ldots, g_{N-1})$.

10.1.1. Aplicación del algoritmo de Hermite en extensiones logarítmicas

A continuación, se aplicará el algoritmo de separación de la integral de Hermite para el caso de extensiones logarítmicas, con algunos cambios pertinentes a las propiedades diferenciales de los objetos, resaltadas en el capítulo 7.

Realizando el algoritmo de la división, existen $P(g_N), r(g_N) \in F_{N-1}[g_N]$ tales que

$$f(g_N) = \frac{p(g_N)}{q(g_N)} = P(g_N) + \frac{r(g_N)}{q(g_N)},$$

donde $r(g_N) = 0$ o $\deg(r(g_N)) < \deg(q(g_N))$. De esta manera,

$$\int f(g_N) = \int P(g_N) + \int \frac{r(g_N)}{q(g_N)}. \tag{10.2}$$

Similar al caso de la integración de funciones racionales, a la integral $\int P(g_N)$ se le llama la parte polinomial de $f(g_N)$, mientras que $\int \frac{r(g_N)}{q(g_N)}$ recibe el nombre de la parte racional. Gracias a los algoritmos ya desarrollados, integrar la parte racional resulta relativamente fácil. En las condiciones actuales, la menos trivial de las dos será la parte polinomial.

Como es de esperarse, se prosigue con el algoritmo de Hermite para integrar la parte racional de $f(g_N)$. En primer lugar, se factora $q(g_N) = \prod_{k=1}^{n} q_k(g_N)^k$ donde cada $q_k(g_N)$ es mónico y libre de cuadrados, con $(q_i(g_N), q_j(g_N)) = 1$ para $i \neq j$, y $\deg(q_k(g_N)) > 0$. Aquí, que $q_k(g_N)$ sea libre de cuadrados es una propiedad en $F_{N-1}[g_N]$, por lo cual $\big(q_k(g_N), D_{g_N}[q_k(g_N)]\big) = 1$. Sin embargo, es posible demostrar también que $\big(q_k(g_N), [q_k(g_N)]'\big) = 1$, como se observa a continuación.

Propiedad 10.1: Sea F un campo diferencial con un símbolo x, donde el operador diferencial $' : F \to F$ es tal que $x' = 1$. Sea $F(g_N)$ una extensión diferencial de F con el mismo campo de constantes, siendo g_N logarítmico y trascendental sobre F. Sea $a(g_N) \in F[g_N]$ mónico con grado positivo, y libre de cuadrados en $F[g_N]$. Entonces, $\big(a(g_N), [a(g_N)]'\big) = 1$.

Demostración. Del teorema 7.2 sobre derivadas de polinomios con entradas logarítmicas, se sabe que $[a(g_N)]' \in F[g_N]$. Sea $F(\beta_1, \beta_2, \ldots, \beta_k)$ el campo de descomposición de $a(g_N)$, con lo cual

$$a(g_N) = \prod_{k=1}^{m} (g_N - \beta_k).$$

Entonces, diferenciando con respecto a x, y tomando $g_N' = u'/u$ para $u \in F$, se tiene

$$[a(g_N)]' = \sum_{k=1}^{m} \left(\frac{u'}{u} - \beta_k' \right) \prod_{j \neq k} (g_N - \beta_j). \tag{10.3}$$

Aquí, dado que $a(g_N)$ es libre de cuadrados en $F[g_n]$, se debe cumplir que los β_k son distintos. Supóngase que existe k tal que uno de los coeficientes $\frac{u'}{u} - \beta_k'$ se anule. Esto implicaría que $\beta_k' = g_N'$, lo cual solo puede ocurrir si $g_N - \beta_k \in \mathrm{con}(F(g_N, \beta_1, \ldots, \beta_m))$. Ahora bien, como F y $F(g_N)$ tienen el mismo campo de constantes, entonces es más que claro que $F(\beta_1, \ldots, \beta_m)$ y $F(g_N, \beta_1, \ldots, \beta_m)$ también tienen el mismo campo de constantes, pues cualquier constante que se añada a través de los β_k en un campo se añadirá en el otro. Esto implica que $g_N - \beta_k \in \mathrm{con}(F(\beta_1, \ldots, \beta_m))$, lo cual a su vez implica que $g_N - \beta_k \in F(\beta_1, \ldots, \beta_m)$. Pero $g_N - \beta_k \notin F$, de manera que $g_N - \beta_k$ es un miembro del generado $\langle \beta_1, \ldots, \beta_m \rangle$, lo cual contradice que g_N sea trascendental sobre F dado que dicho generado es un campo de elementos algebraicos.

Solamente queda como posibilidad que para todo k, se tenga $\frac{u'}{u} - \beta_k' \neq 0$. Como se observa en la ecuación 10.3, esto implica que $[a(g_N)]'$ posee $m-1$ términos divisibles por cualquier $g_N - \beta_k$, y un solo término que no es divisible por $g_N - \beta_k$. Entonces, es claro que $a(g_N)$ y $[a(g_N)]'$ no poseen factores comunes, demostrando el resultado.

■

Este resultado será de utilidad para continuar el uso del teorema de Hermite, pues es necesario transformar la derivada con respecto a g_N en una derivada con respecto a x.

Retomando donde nos quedamos, es posible realizar una descomposición en fracciones parciales para la parte racional utilizando los factores libres de cuadrados del denominador, y se obtiene que

$$\int \frac{r(g_N)}{q(g_N)} = \int \frac{r(g_N)}{\prod_{k=1}^{n} q_k(g_N)^k} = \sum_{k=1}^{n} \sum_{j=1}^{k} \int \frac{r_{k_j}(g_N)}{q_k(g_N)^j},$$

donde $r_{k_j}(g_N) \in F_{N-1}[g_N]$, y $\deg(r_{k_j}(g_N)) < \deg(q_k(g_N))$ cuando $\deg(q_k(g_N)) > 0$, pero además $r_{k_j}(g_N) = 0$ cuando $q_k(g_N) = 1$. A partir de aquí, gracias a la propiedad 10.1, se cumplen con los supuestos necesarios para aplicar los siguientes pasos del algoritmo de Hermite vistos en el teorema 8.1, de manera que existen polinomios $s(g_N), t(g_N) \in F_{N-1}[g_N]$ para los cuales se calcula

$$\int \frac{r_{k_j}(g_N)}{q_k(g_N)^j} = -\frac{1}{j-1} \frac{t(g_N)}{q_k(g_N)^{j-1}} + \frac{1}{j-1} \int \frac{(j-1)s(g_N) + [t(g_N)]'}{q_k(g_N)^{j-1}}.$$

Nótese que la diferenciación de logaritmos mantiene el grado o lo disminuye en 1, por lo cual

$$\deg\left(s(g_N) + \frac{1}{j-1} [t(g_N)]' \right) \leq \deg(q_k(g_N)).$$

Luego, las condiciones para el algoritmo de Hermite aún aplican siempre y cuando $j - 1 > 1$, y se detiene el algoritmo cuando $j - 1 = 1$. En ese caso, se logró expresar la integral original como

$$\int \frac{r(g_N)}{q(g_N)} = \frac{c(g_N)}{d(g_N)} + \int \frac{a(g_N)}{b(g_N)},$$

donde $\deg(a(g_N)) < \deg(b(g_N))$, siendo $b(g_N)$ mónico y libre de cuadrados, y todos estos polinomios siendo parte de $F_{N-1}[g_N]$. Todo lo que queda es integrar esta última expresión $a(g_N)/b(g_N)$ en el campo $F_{N-1}(g_N)$. Con este propósito en mente, debemos demostrar que la función racional $a(g_N)/b(g_N)$ cumple con todos los supuestos requeridos por los teoremas de Rothstein-Trager.

10.1.2. Rothstein-Trager en la extensión logarítmica

Debido a que las condiciones algebraicas y diferenciales sobre el campo en el cual se encuentra el integrando ahora son distintas, no es posible aplicar los teoremas de Rothstein-Trager sin antes asegurarnos que los supuestos del mismo se cumplan. Por ejemplo, al definir el resultante correspondiente al símbolo g_N, se obtiene el polinomio

$$R(z) = \operatorname{res}_{g_N} \big(a(g_N) - z[b(g_N)]', b(g_N)\big) \in F_{N-1}[z],$$

cuyas raíces no necesariamente son constantes respecto a x o a g_N. Esto conlleva a cambios importantes en el algoritmo de Rothstein-Trager para el caso de extensiones logarítmicas, llevándonos al primer teorema de caracterización de antiderivadas elementales. Este teorema junta los tres teoremas de Rothstein-Trager en uno solo, pues las demostraciones esta vez pueden tomarse de la mano aprovechando las versiones demostradas en el capítulo 8.

Teorema 10.1 (Rothstein-Trager para funciones logarítmicas)**:** Sea F un campo de funciones elementales y $K = \operatorname{con}(F)$. Sea g trascendental y logarítmico sobre F, con $g = \log(u)$ para $u \in F$. Supóngase también que la extensión elemental trascendental $F(g)$ tiene el mismo campo de constantes que F. Considérese $a(g), b(g) \in F[g]$ con $\big(a(g), b(g)\big) = 1$, con $\deg(a(g)) < \deg(b(g))$, y con $b(g)$ mónico y libre de cuadrados. Defínase, adicionalmente,

$$R(z) = \operatorname{res}_g \big(a(g) - z[b(g)]', b(g)\big) \in F[z],$$

con raíces c_k para $1 \leq k \leq m$. Además, se definen

$$v_k(g) = \big(a(g) - c_k[b(g)]', b(g)\big) \in F(c_1, \ldots, c_m)[g],$$

de manera que se cumple:

- $\displaystyle\int \frac{a(g)}{b(g)}$ es elemental si y solo si las raíces de $R(z) \in F[z]$ son constantes no todas nulas.
- Si $\displaystyle\int \frac{a(g)}{b(g)}$ es elemental, entonces se da la representación $\displaystyle\frac{a(g)}{b(g)} = \sum_{k=1}^{m} c_k \frac{[v_k(g)]'}{v_k(g)}$, o bien:

$$\int \frac{a(g)}{b(g)} = \sum_{k=1}^{m} c_k \log(v_k(g)).$$

- Si F^* es la mínima extensión algebraica de F tal que se cumple el enunciado anterior, entonces debe darse que $F^* = F(c_1, c_2, \ldots, c_m)$.

Demostración. Supóngase que $\int \frac{a(g)}{b(g)}$ es elemental. Entonces, por el principio de Liouville,

$$\frac{a(g)}{b(g)} = [v_0(g)]' + \sum_{k=1}^{m} c_k \frac{[v_k(g)]'}{v_k(g)},$$

para $c_k \in K^*$ y $v_k(g) \in F^*(g)$, siendo K^* la mínima extensión de K necesaria para expresar la integral y F^* la extensión de F tal que $\mathrm{con}(F^*) = K^*$. Puede asumirse sin perder la generalidad que los $v_k(g)$ son polinomios mónicos en $F^*[g]$ usando las propiedades de suma y resta de logaritmos, las cuales aplican dado que aparecen en la forma $[v_k(g)]'/v_k(g)$. Como se hizo en Rothstein-Trager para funciones racionales, también puede asumirse que los c_k son distintos y no nulos, y que los $v_k(g)$ son libres de cuadrados y primos relativos por pares.

Estos argumentos no necesariamente funcionan para $v_0(g)$, dado que no es el argumento de un logaritmo. Entonces, supóngase que $v_0(g) = p_0(g)/q_0(g)$ para $p_0(g)$ y $g_0(g)$ polinomios primos relativos en $F^*[g]$, con $\deg(q_0(g)) > 0$. Como se argumenta en el teorema de Liouville, esto implica que $[v_0(g)]'$ posee al menos un factor en el denominador que no es libre de cuadrados, como se puede observar en la ecuación 9.4. Pero $b(g)$ por su parte sí es libre de cuadrados, por lo cual esto es imposible. Por lo tanto, es necesario que también $v_0(g) \in F^*[g]$. Debido al teorema de diferenciación de polinomios logarítmicos, entonces $[v_0(g)]' \in F^*[g]$. De ser no nulo, a la hora de obtener un denominador común en la expresión inicial para $a(g)/b(g)$ el numerador tendrá un grado mayor al del denominador. Pero $\deg(a(g)) < \deg(b(g))$, de lo cual es necesario que $[v_0(g)]' = 0$. Esto es,

$$\frac{a(g)}{b(g)} = \sum_{k=1}^{m} c_k \frac{[v_k(g)]'}{v_k(g)} \implies \int \frac{a(g)}{b(g)} = \sum_{k=1}^{m} c_k \log(v_k(g)).$$

Sin embargo, queda por mostrar que los c_k y los v_k cumplen su asociación al resultante. A través de exactamente el mismo argumento de Rothstein-Trager para funciones racionales, se llega a que

$$b(g) \mid \prod_{k=1}^{m} v_k(g), \qquad \prod_{k=1}^{m} v_k(g) \mid b(g).$$

Y como todos estos polinomios son mónicos, se tiene $b(g) = \prod_{k=1}^{m} v_k(g)$. A partir de aquí, todos los argumentos son análogos a los de la prueba de Rothstein-Trager en el caso racional simple. Por lo tanto, es claro que queda demostrado el segundo punto, pues los $v_k(g)$ tendrán la forma deseada, por el teorema 8.3). También queda demostrado el tercer punto, pues se asumió que se trabajaba sobre el campo de constantes mínimo, aplicando entonces el teorema 8.4. Para el primer punto, también queda demostrada la implicación de necesidad, pues se supuso que la integral es elemental, y el teorema 8.3 dice que las constantes c_k son los ceros del resultante y los coeficientes frente a los logaritmos en la solución elemental de la integral. Así, únicamente queda por demostrar la suficiencia: que si los ceros del resultante son constantes, entonces la integral es elemental.

Supóngase que todas las raíces de $R(z)$ son constantes, y sean estas c_k para $1 \leq k \leq m$, ignorando las raíces múltiples. Defínanse también $v_k(g) = (a(g) - c_k[b(g)]', b(g)) \in F(c_1, \ldots, c_m)[g]$ correspondientes a cada c_k. Si $i \neq j$, entonces $(v_i(g), v_j(g))$ divide tanto a $a(g) - c_i[b(g)]'$, como a $a(g) - c_j[b(g)]'$ y a $b(g)$ por definición. Restando, se sigue $(v_i(g), v_j(g)) \mid (c_i - c_j)[b(g)]'$. Así, $b(g)$ y $[b(g)]'$ presentan un factor común en $(v_i(g), v_j(g))$. Sin embargo $b(g)$ es libre de cuadrados, por lo cual se requiere $(v_i(g), v_j(g)) = 1$. Esto es, los $v_k(g)$ son primos relativos por pares.

Ahora, dado que $v_k(g) = (a(g) - c_k[b(g)]', b(g))$, debe darse entonces $v_k(g) \mid b(g)$ para cada k, de manera que existe un polinomio $w(g) \in F(c_1, \ldots, c_m)[g]$ tal que

$$b(g) = w(g) \prod_{k=1}^{m} v_k(g).$$

Supóngase que $\deg(w(g)) > 0$. Entonces, $\text{res}_g(a(g) - z[b(g)]', w(g)) \in F[z]$ es un polinomio con grado no nulo por el criterio de Sylvester. Sea z_0 una raíz de este. Luego, es posible observar que

$$(a(g) - z_0[b(g)]', w(g)) \mid (a(g) - z_0[b(g)]', b(g)).$$

Dado que $(a(g) - z[b(g)]', w(g))$ no es constante, entonces $\text{res}_g(a(g) - z_0[b(g)]', b(g)) = 0$, de nuevo por criterio de Sylvester. De la definición de $R(z)$, esto implica que $z_0 = c_k$ para algún k. Pero entonces, $(a(g) - z_0[b(g)]', w(g))$ es un factor común no trivial de $w(g)$ y de $v_k(g)$, de manera que

$$\left(w(g), \prod_{k=1}^{m} v_k(g) \right) \neq 1,$$

lo cual contradice que $b(g)$ sea libre de cuadrados. Así, es necesario que $\deg(w(g)) = 0$, y debido a que $b(g)$ y los $v_k(g)$ son mónicos, entonces $w(g) = 1$. Una vez más, se llegó a la expresión esperada $b(g) = \prod_{k=1}^{m} v_k(g)$. Diferenciando el producto,

$$[b(g)]' = \sum_{k=1}^{m} [v_k(g)]' \prod_{j \neq k} v_j(g).$$

Ahora bien, defínase un polinomio $\overline{a}(g) \in F[g]$, el cual tenga la forma

$$\overline{a}(g) = \sum_{k=1}^{m} c_k [v_k(g)]' \prod_{j \neq k} v_j(g).$$

Por lo tanto, para cada posible $1 \leq i \leq m$, se tiene

$$\overline{a}(g) - c_i[b(g)]' = \sum_{k=1}^{m} (c_k - c_i)[v_k(g)]' \prod_{j \neq k} v_j(g).$$

Cuando k pasa por el índice i, entonces $c_k - c_i$ se anula, y ese sería el único momento posible en el cual v_i no podría aparecer como factor en un término de $\overline{a}(g) - c_i[b(g)]'$. Por lo tanto, es claro que

$$v_i(g) \mid \overline{a}(g) - c_i[b(g)]'$$

para todo i en $1 \leq i \leq m$. Además, $v_i(g) \mid a(g) - c_i[b(g)]'$ también para cada índice por definición. Restando las divisibilidades, queda claro que $v_i(g) \mid a(g) - \overline{a}(g)$. Pero entonces, dado que los $v_k(g)$ son primos relativos por pares y su producto es $b(g)$, se llega a que $b(g) \mid a(g) - \overline{a}(g)$. Siendo $b(g)$ una multiplicación de m factores $v_k(g)$, siendo $\overline{a}(g)$ una suma de multiplicaciones de $m-1$ factores $v_k(g)$ y un factor $[v_k(g)]'$, y debido a que $\deg([v_k(g)]') < \deg(v_k(g))$ gracias a que los $v_k(g)$ son mónicos, entonces $\deg(\overline{a}(g)) < \deg(b(g))$. También $\deg(a(g)) < \deg(b(g))$ por hipótesis, lo cual implica que $\deg(a(g) - \overline{a}(g)) < \deg(b(g))$. Pero entonces $b(g)$ solo puede dividir a $a(g) - \overline{a}(g)$ si este último es cero. Es decir, $a(g) = \overline{a}(g)$. De esta manera,

$$\frac{a(g)}{b(g)} = \frac{\sum_{k=1}^{m} c_k [v_k(g)]' \prod_{j \neq k} v_j(g)}{\prod_{k=1}^{m} v_k(g)} = \sum_{k=1}^{m} c_k \frac{[v_k(g)]'}{v_k(g)}.$$

En otras palabras, la integral es elemental debido a que posee la representación

$$\int \frac{a(g)}{b(g)} = \sum_{k=1}^{m} c_k \log(v_k(g)).$$

■

Este teorema facilitará demostrar que una gran cantidad de antiderivadas no son elementales, y también nos proporciona un algoritmo para encontrar las antiderivadas que sí son elementales. A continuación, observamos una gran cantidad de ejemplos.

Ejemplo 10.1: La función logaritmo integral.

Considérense las funciones

$$\operatorname{li}(t) = \int_0^t \frac{1}{\log(x)}\,\mathrm{d}x\,, \qquad\qquad \operatorname{Li}(t) = \int_2^t \frac{1}{\log(x)}\,\mathrm{d}x\,.$$

Estas reciben el nombre de *logaritmo integral* y *logaritmo integral desplazado*, respectivamente. Una definición algebraica de este tipo de funciones se presenta en el Anexo 14.2. Su relevancia es alta en la teoría de números, donde aparece como una aproximación asintótica a la función contadora de números primos. Resulta que su integrando no posee antiderivada elemental.

Demostración. Considérese $g = \log(x)$, de manera que el integrando $f = 1/g$ se encuentra en el campo $K(x, g)$, siendo K cualquier subcampo de $\mathbb{C}$. De esta manera, usando la notación del teorema 10.1, se tiene $a(g) = 1$ y $b(g) = g$, con lo cual

$$R(z) = \operatorname{res}_g\left(a(g) - z[b(g)]', b(g)\right) = \operatorname{res}_g\left(1 - \frac{z}{x}, g\right) = 1 - \frac{z}{x}.$$

De esta manera, $R(z) = 0$ se cumple cuando $z = x$, con lo cual los ceros del resultante son no constantes en $K(x, g)$. Así, resulta que el integrando dado no posee antiderivada elemental.

■

Algunos de los ejemplos a continuación son casos generales de este ejemplo.

Ejemplo 10.2: Logaritmos anidados en el denominador. Considérense funciones del siguiente tipo:

$$\int \frac{1}{\log(\log(x))}\,\mathrm{d}x\,, \qquad \int \frac{1}{\log(\log(\log(x)))}\,\mathrm{d}x\,, \qquad \int \frac{1}{\log(\log(\log(\log(x))))}\,\mathrm{d}x\,.$$

Estas antiderivadas siempre son no elementales.

Demostración. Para su representación, se presenta la sucesión iniciada en $g_1 = \log(x)$, y con regla de asignación del sucesor $g_k = \log(g_{k-1})$. De esta manera, se tiene:

$$g_1' = \frac{1}{x}, \qquad g_2' = \frac{g_1'}{g_1} = \frac{1}{x\log(x)} = \frac{1}{xg_1}, \qquad g_3' = \frac{g_2'}{g_2} = \frac{1}{x\log(x)\log(\log(x))} = \frac{1}{xg_1g_2}, \qquad \cdots.$$

Como hipótesis inductiva, supóngase que se cumple

$$g_{n-1}' = \frac{1}{xg_1g_2\cdots g_{n-2}}.$$

Entonces, para g_n se sigue que también

$$g_n' = \frac{g_{n-1}'}{g_{n-1}} = \frac{1}{xg_1g_2\cdots g_{n-2}g_{n-1}}.$$

Con esto, podemos asegurar que esta es la forma general de g_n'. Ahora bien, considérese la integral

$$\int \underbrace{\frac{1}{\log(\log(\cdots\log(x)))}}_{n \text{ iteraciones del logaritmo}}\,\mathrm{d}x = \int \frac{1}{g_n}\,\mathrm{d}x\,.$$

Entonces, es claro que el integrando pertenece a $K(x, g_1, g_2, \ldots, g_n)$, con la sucesión de funciones definida. Con esto, se tiene $a(g_n) = 1$ y $b(g_n) = g_n$, de manera que

$$R(z) = \operatorname{res}_{g_n}\left(a(g_n) - z[b(g_n)]', b(g_n)\right) = \operatorname{res}_{g_n}\left(1 - \frac{z}{xg_1g_2\cdots g_{n-1}}, g_n\right) = 1 - \frac{z}{xg_1g_2\cdots g_{n-1}}.$$

De esta manera, $R(z) = 0$ se cumple cuando $z = xg_1 g_2 \cdots g_{n-1}$, que claramente no es constante en $K(x, g_1, g_2, \ldots, g_{n-1})$. Por lo tanto, independiente de la cantidad de logaritmos anidados, las integrales de esta forma nunca tienen antiderivada elemental.

■

Ejemplo 10.3: Desplazamiento por un polinomio.

Sea $p(x) \in K[x]$, donde K es un subcampo de $\mathbb{C}$. Las integrales siguientes siempre son no elementales:

$$\int \frac{1}{p(x) + \log(x)}\, \mathrm{d}x\,.$$

Demostración. Claramente, este integrando se encuentra en $K(x, \log(x))$, y cumple las hipótesis del teorema 10.1. Tomando $g = \log(x)$, se tiene $a(g) = 1$ y $b(g) = p(x) + g$. Así, $[b(g)]' = p'(x) + 1/x$, y

$$R(z) = \mathrm{res}_g \left(a(g) - z[b(g)]', b(g)\right) = \mathrm{res}_g \left(1 - zp'(x) - \frac{z}{x}, g\right) = 1 - zp'(x) - \frac{z}{x}.$$

Luego, $R(z) = 0$ implica que $x - xp'(x)z - z = 0$, con lo cual

$$z = \frac{x}{xp'(x) + 1} = \frac{1}{p'(x) + 1/x}.$$

Es claro que $z \notin K$ para cualquier posible $p'(x) \in K[x]$, de manera que la antiderivada es no elemental, independiente del polinomio que se escoja.

■

Ejemplo 10.4: Generalizaciones en potencias.

Considérese una integral del tipo

$$\int \frac{x^m}{[\log(x)]^a}\, \mathrm{d}x\,,$$

donde $m \in K$ y $a \in \mathbb{Z}^+$. Independiente del valor de a, esta integral es elemental cuando $m = -1$, y es no elemental cuando $m \neq -1$.

Demostración. Este integrando no cumple el supuesto de libertad de cuadrados en general, solo cuando $a = 1$. Tomemos entonces el caso $a = 1$ como base. Se toma $g = \log(x)$, de manera que se usa el campo $K(x, g)$, y la función actualmente tiene la forma x^m/g. Así,

$$R(z) = \mathrm{res}_g \left(x^m - \frac{z}{x}, g\right) = x^m - \frac{z}{x}.$$

Así, $R(z) = 0$ solo cuando $z = x^{m+1}$. Nótese que esto es constante únicamente cuando $m = -1$. Por lo tanto, la integral de $x^m/\log(x)$ es elemental si $m = -1$, pero es no elemental en cualquier otro caso. En el caso de elementalidad, se tiene que $c_1 = 1$ es la única raíz, y

$$v_1(g) = \left(\frac{1}{x} - \frac{1}{x}, \log(x)\right) = (0, \log(x)) = \log(x).$$

Por lo tanto, en este caso particular, el algoritmo produce la antiderivada

$$\int \frac{1}{x \log(x)}\, \mathrm{d}x = \log(\log(x)).$$

Ahora, continuemos con el caso $a > 0$ y $m \neq -1$. Nótese que,

$$\int \frac{x^m}{[\log(x)]^a}\, \mathrm{d}x = \int \frac{x^{m+1}}{x[\log(x)]^a}.$$

De esta manera, es posible realizar integración por partes utilizando $u = x^{m+1}$ y $\mathrm{d}v = \dfrac{1}{x[\log(x)]^a}\,\mathrm{d}x$:

$$\int \frac{x^m}{[\log(x)]^a}\,\mathrm{d}x = \frac{x^{m+1}}{(1-a)[\log(x)]^{a-1}} - \frac{m+1}{1-a}\int \frac{x^m}{[\log(x)]^{a-1}}\,\mathrm{d}x\,.$$

Si se diera el caso en que $a - 1 = 1$, entonces se usa el resultado anterior para argumentar que esta última integral no es elemental. Si $a - 1 \neq 1$, se vuelve a realizar esta estrategia, hasta que el exponente de $\log(x)$ sea 1. Por tanto, todas estas integrales dependen del caso $a = 1$. Así, queda demostrado que la integral dada es no elemental siempre que $m \neq -1$ y $a \in \mathbb{Z}^+$.

Cuando $m = -1$, la integral sí es elemental, y se tiene

$$\int \frac{1}{x\log(x)}\,\mathrm{d}x = \log(\log(x)), \qquad \int \frac{1}{x[\log(x)]^a}\,\mathrm{d}x = \frac{x^{m+1}}{(1-a)[\log(x)]^{a-1}},$$

dependiendo de si $a = 1$ o $a \neq 1$.

■

Nota Bene 10.1: Sustitución de funciones.

Considérese el ejemplo 10.4. Sea $u = \log(x)$, y realice sustitución como se haría en cálculo. De esta manera $x = e^u$, y $\mathrm{d}x = e^u\,\mathrm{d}u$. Luego,

$$\int \frac{x^m}{[\log(x)]^a}\,\mathrm{d}x = \int \frac{e^{(m+1)u}}{u^a}\,\mathrm{d}u\,.$$

Entonces, la integral exponencial en la derecha es no elemental cuando $m + 1 \neq 0$ y $a \in \mathbb{Z}^+$. ¿Cuál es la necesidad, entonces, de trabajar por separado los casos de integrandos en campos diferenciales con extensiones logarítmicas y extensiones exponenciales?

En el presente desarrollo de la teoría del álgebra diferencial, no se ha formalizado el concepto de sustitución de funciones. De hecho, incluso la composición de funciones se ha tratado como un tema bastante lejano, únicamente apareciendo a la hora de adjuntar nuevas funciones a un campo. Por esta falta de herramientas, resulta necesario tratar los casos como separados. Sin embargo, una unificación de ambas teorías podría resultar en un desarrollo interesante del álgebra diferencial.

Estos ejemplos dan una idea de lo poderosos que son los teoremas de Rothstein-Trager, incluso cuando la hipótesis de dichos teoremas es tan exigente. A continuación, se resuelve por completo el problema de integración en extensiones logarítmicas, a través de la integración de la parte polinomial.

10.1.3. Sobre la integración de la pieza polinomial logarítmica

Por ahora, se ha llegado a un resultado bastante útil para determinar si las antiderivadas de funciones racionales en extensiones logarítmicas elementales que satisfacen los requerimientos de Rothstein-Trager son, o no son, elementales. Es más, este resultado permite encontrar la antiderivada en caso sí sea elemental. Sin embargo, es hora de discutir qué ocurre con la pieza polinomial.

A través del uso del algoritmo de la división en $F_{N-1}[g_N]$, se llegó a la ecuación 10.2, donde nos interesa integrar $\int P(g_N)$. Aquí, $P(g_N) \in F_{N-1}[g_N]$, y por lo tanto tomando $\deg(P) = \lambda$ y $P_k \in F_{N-1}$ es posible escribir

$$P(g_N) = \sum_{k=0}^{\lambda} P_k g_N^k.$$

Esta será la forma del polinomio general que se trabajará. Ahora, se demuestra el teorema a continuación, que resuelve por completo el problema de integración de polinomios logarítmicos.

Teorema 10.2: Sea F un campo de funciones elementales y $K = \mathrm{con}(F)$. Sea g trascendental y logarítmica sobre F, con $g = \log(u)$ para $u \in F$. Supóngase también que la extensión elemental trascendental $F(g)$ tiene el mismo campo de constantes que F. Sea $P(g) \in F[g]$ con $\deg(P(g)) = \lambda$ y coeficientes P_k para $0 \leq k \leq \lambda$. Sea además $\overline{K}$ la cerradura algebraica de K, y $\overline{F}$ la extensión de F tal que $\mathrm{con}(\overline{F}) = \overline{K}$. Si $\int P(g)$ es elemental, entonces existen funciones $q_k \in \overline{F}$ para $1 \leq k \leq \lambda + 1$, y una función $\overline{q_0}$ en una extensión logarítmica de $\overline{F}$ tales que

$$\int P(g) = \overline{q_0} + \sum_{k=1}^{\lambda+1} q_k g^k.$$

Las funciones q_k y $\overline{q_0}$ satisfacen el sistema de $\lambda + 2$ ecuaciones por $\lambda + 2$ variables:

$$\begin{cases} 0 & = q'_{\lambda+1}, \\ P_\lambda & = (\lambda+1)g' q_{\lambda+1} + q'_\lambda, \\ P_{\lambda-1} & = \lambda g' q_\lambda + q'_{\lambda-1}, \\ & \vdots \\ P_1 & = 2g' q_2 + q'_1, \\ P_0 & = g' q_1 + \overline{q_0}'. \end{cases}$$

Dicho sistema puede solucionarse recursivamente.

Demostración. De ser $\int P(g_N)$ elemental, se tiene por principio de Liouville

$$P(g_N) = [v_0(g_N)]' + \sum_{k=1}^{m} c_k \frac{[v_k(g_N)]'}{v_k(g_N)},$$

donde los c_k son constantes posiblemente añadidas a K, y los $v_k(g_N)$ son funciones posiblemente en una extensión de $F_{N-1}[g_N]$ con las nuevas constantes añadidas a K. Sean $\overline{K}$ y $\overline{F}_{N-1}$ estas extensiones. Como en la prueba del teorema de Liouville, será necesario que los v_k se independan de g_N para $k \neq 0$. Así, se tendrá $c_k \in \overline{K}$, $v_0(g_N) \in \overline{F}_{N-1}[g_N]$, y $v_k \in \overline{F}_{N-1}$ para $k \neq 0$, con lo cual

$$P(g_N) = [v_0(g_N)]' + \sum_{k=1}^{m} c_k \frac{v'_k}{v_k}. \tag{10.4}$$

Ahora, escríbase $v_0(g_N) = \sum_{k=0}^{\mu} q_k g_N^k$, para $q_k \in \overline{F}_{N-1}$. Del teorema de diferenciación de polinomios logarítmicos, $[v_0(g_N)]' \in \overline{F}_{N-1}[g_N]$ y $\deg([v_0(g_N)]') = \mu - 1$ o $\deg([v_0(g_N)]') = \mu$, dependiendo de si $q_\mu \in \overline{K}$. De cualquier manera, el máximo grado posible para $v_0(g_N)$ es $\mu = \lambda + 1$. Entonces, la ecuación 10.4 se convierte en

$$\sum_{k=0}^{\lambda} P_k g_N^k = \left(\sum_{k=0}^{\lambda+1} q_k g_N^k \right)' + \sum_{k=1}^{m} c_k \frac{v'_k}{v_k} \implies \sum_{k=0}^{\lambda} P_k g_N^k = \sum_{k=1}^{\lambda+1} (q'_k g_N^k + k q_k g_N^{k-1} g'_N) + q'_0 + \sum_{k=1}^{m} c_k \frac{v'_k}{v_k}.$$

Definiendo $\overline{q_0} = q_0 + \sum_{k=1}^{m} c_k \log(v_k)$, al igualar coeficientes, se genera el sistema de $\lambda+2$ ecuaciones con $\lambda + 2$ incógnitas en $\overline{q_0}$ y los q_k para $1 \leq k \leq \lambda + 1$:

$$\begin{cases} 0 & = q'_{\lambda+1}, \\ P_\lambda & = (\lambda+1)g'_N q_{\lambda+1} + q'_\lambda, \\ P_{\lambda-1} & = \lambda g'_N q_\lambda + q'_{\lambda-1}, \\ & \vdots \\ P_1 & = 2g'_N q_2 + q'_1, \\ P_0 & = g'_N q_1 + \overline{q_0}'. \end{cases}$$

Los coeficientes $P_k \in F_{N-1}$ son conocidos, al igual que g'_N. Se busca determinar las soluciones $q_k \in \overline{F}_{N-1}$ y $\overline{q_0} \in \overline{F}_{N-1}(\log(v_1), \ldots, \log(v_m))$. Esto servirá como herramienta, pues los q_k se encuentran dentro del campo diferencial original completado con las constantes necesarias, y $\overline{q_0}$ se encuentra en una extensión logarítmica del campo diferencial original.

Integrando la primera ecuación, es claro que $q_{\lambda+1} = b_{\lambda+1} \in \overline{K}$. Cabe recalcar que para cada q_k hay una constante de integración b_k asociada a ella, lo cual será aparente en el proceso recursivo a continuación. Ahora, en la segunda ecuación, se tiene

$$\int P_\lambda = \int \left((\lambda+1)b_{\lambda+1}g'_N + q'_\lambda\right) = (\lambda+1)b_{\lambda+1}g_N + q_\lambda + b_\lambda \tag{10.5}$$

Se desea encontrar una expresión para la constante $b_{\lambda+1}$ y la función q_λ. Para ello, es necesario que $\int P_\lambda$ sea elemental, que aparezca como máximo una extensión logarítmica en la integral por el teorema 9.1, y que esta esté dada por g_N. De fallar **una** de estas condiciones, es posible concluir inmediatamente que $\int P(g_N)$ es no elemental, pues se incumpliría el principio de Liouville. Suponiendo que las condiciones se cumplen para P_λ, entonces

$$\int P_\lambda = c_\lambda g_N + d_\lambda, \tag{10.6}$$

para $c_\lambda \in \overline{K}$ y $d_\lambda \in \overline{F}_{N-1}$. Igualando las ecuaciones 10.5 y 10.6, salvo una constante de integración $b_\lambda \in \overline{K}$, se deduce que

$$b_{\lambda+1} = \frac{c_\lambda}{\lambda+1}, \qquad\qquad q_\lambda = d_\lambda + b_\lambda.$$

Este tipo de sustitución puede seguirse realizando, aunque no resulte inmediato. En la tercera ecuación, se obtiene

$$P_{\lambda-1} = \lambda g'_N(d_\lambda + b_\lambda) + q'_{\lambda-1},$$

lo cual puede reescribirse usando que $g_N = \log(u)$ para $u \in F_{N-1}$ como

$$\int \left(P_{\lambda-1} - \frac{\lambda d_\lambda u'}{u}\right) = \lambda b_\lambda g_N + q_{\lambda-1} + b_{\lambda-1}.$$

Pero, dado que el integrando en esta ecuación pertenece a $\overline{F}_{N-1}$ de la misma manera que P_λ, podemos invocar el mismo argumento garantizado por el principio de Liouville. Esto es, de poseer antiderivada elemental, existen $c_{\lambda-1} \in \overline{K}$ y $d_{\lambda-1} \in \overline{F}_{N-1}$ para los cuales la antiderivada tiene la forma $c_{\lambda-1}g_N + d_{\lambda-1}$. Luego, es claro que

$$b_\lambda = \frac{c_{\lambda-1}}{\lambda}, \qquad\qquad q_{\lambda-1} = d_{\lambda-1} + b_{\lambda-1}.$$

A partir de aquí, se vuelve aparente que este proceso puede seguirse recursivamente hasta llegar a las últimas ecuaciones. En general, será posible escribir

$$\int \left(P_{k-1} - \frac{k d_k u'}{u}\right) = k b_k g_N + q_{k-1} = c_{k-1}g_N + d_{k-1} + b_{k-1}, \tag{10.7}$$

para $2 \le k \le \lambda$, de manera que para dichos índices se tiene

$$b_k = \frac{c_{k-1}}{k}, \qquad\qquad q_{k-1} = d_{k-1} + b_{k-1}. \tag{10.8}$$

Así, el sistema de ecuaciones está prácticamente resuelto, faltando únicamente utilizar la última ecuación para encontrar $\overline{q_0}$. Sustituyendo la expresión correspondiente para q_1, y reescribiendo como en la ecuación 10.7, se tendrá

$$\int \left(P_0 - \frac{d_1 u'}{u}\right) = b_1 g_N + \overline{q_0}.$$

De nuevo, si esta integral fuese no elemental, la integral completa tampoco lo sería. Supóngase entonces que sí lo es. Escríbase la misma como d_0, pues las extensiones logarítmicas ya fueron tomadas en cuenta en el $\overline{q_0}$. De esta manera, obtenemos una expresión para la última incógnita en $\overline{q_0} = d_0 - b_1 g_N + b_0$. Pero $\int P(g_N)$ absorbe la constante b_0 en su clase de equivalencia, así que podemos ignorarla. Además, al ser $q_1 = d_1 + b_1$, entonces el término en la representación de la integral es $q_1 g_N = d_1 g_N + b_1 g_N$. De esta manera, b_1 tampoco toma importancia, pues $\overline{q_0} + q_1 g_N = d_0 + d_1 g_N$ al cancelarse el término $b_1 g_N$. Podemos, entonces, asumir siempre que dicho término es nulo.

■

A continuación, vemos algunos ejemplos de uso del teorema 10.2.

Ejemplo 10.5: Logaritmos anidados.

La antiderivada de n logaritmos anidados, con $n \geq 2$, siempre es no elemental.

Demostración. Considérese primero la anidación de únicamente dos logaritmos:

$$\int \log(\log(x))\,\mathrm{d}x\,.$$

Claramente, $g = \log(\log(x)) \in K(x, \log(x), \log(\log(x)))$. De esta manera, se desea integrar el polinomio lineal $P(g) = g$ sobre el campo $F = K(x, \log(x))$. Así,

$$\int g = b_2 g^2 + q_1 g + \overline{q_0}.$$

Para b_2, q_1 y $\overline{q_0}$, se deben cumplir las ecuaciones

$$\begin{cases} 0 = b_2', \\ 1 = 2b_2 g' + q_1', \\ 0 = g' q_1 + \overline{q_0}'. \end{cases}$$

De la primera ecuación, únicamente es claro que b_2 es una constante. De la segunda, al integrar se obtiene $x = 2b_2 g + q_1$, ignorando b_1 como en la prueba del teorema 10.2. El lado izquierdo no depende del logaritmo g, haciendo necesario que $b_2 = 0$ y $q_1 = x$. Ahora, la tercera ecuación produce

$$0 = g'x + \overline{q_0}' \implies 0 = \frac{x}{x\log(x)} + \overline{q_0}' = \frac{1}{\log(x)} + \overline{q_0}'.$$

Integrando esta ecuación, e ignorando la última constante de integración b_0 tomando la clase de equivalencia, se tiene

$$\overline{q_0} = -\int \frac{1}{\log(x)}\,\mathrm{d}x\,.$$

La integral sin resolver corresponde al ejemplo 10.1, la función logaritmo integral, la cual se demostró que no es elemental. Al aparecer en su expansión, la antiderivada de $\log(\log(x))$ tampoco es elemental. Sin embargo, se obtiene

$$\int \log(\log(x))\,\mathrm{d}x = x\log(\log(x)) - \int \frac{1}{\log(x)}\,\mathrm{d}x\,.$$

Es decir, la antiderivada depende de la función no elemental que aparece en el ejemplo 10.1. Por otro lado, aprovechando la linealidad de la integral, esto también nos da el resultado

$$\int \left(\log(\log(x)) + \frac{1}{\log(x)}\right)\mathrm{d}x = x\log(\log(x)).$$

Ahora, se procede a realizar el trabajo para una iteración de más de dos logaritmos. Es decir, se busca encontrar antiderivadas del siguiente tipo:

$$\int \log(\log(\log(x)))\,\mathrm{d}x\,, \qquad \int \log(\log(\log(\log(x))))\,\mathrm{d}x\,, \qquad \int \underbrace{\log(\log(\cdots\log(x)))}_{n \text{ iteraciones del logaritmo}}\,\mathrm{d}x\,.$$

Se toma la sucesión iniciada en $g_1 = \log(x)$, y con regla de asignación del sucesor $g_k = \log(g_{k-1})$, como se hizo en el ejemplo 10.2. En este caso, ya se conocen las propiedades diferenciales de los g_k. La función a integrar será g_n, la anidación de n logaritmos. Esta se encuentra en $K(x, g_1, \ldots, g_n)$. Puesto que $P(g_n) = g_n$ es el mismo polinomio lineal, se usa el mismo sistema de ecuaciones del caso de 2 iteraciones del logaritmo. Así, de la tercera ecuación se obtiene

$$0 = \frac{x}{x g_1 g_2 \cdots g_{n-2} g_{n-1}} + \overline{q_0}' \implies 0 = \frac{1}{g_1 g_2 \cdots g_{n-2} g_{n-1}} + \overline{q_0}'.$$

De aquí, se llega a

$$\overline{q_0} = -\int \frac{1}{g_1 g_2 \cdots g_{n-2} g_{n-1}}.$$

Sin embargo, a diferencia del caso de $\log(\log(x))$, aún no se ha demostrado la no-elementalidad de la integral que aún aparece en esta expansión. Para ello, se toma $F = K(x, g_1, \ldots, g_{n-1})$, de manera que se integra sobre $F(g_n)$. Así, será posible utilizar el teorema 10.1 de Rothstein-Trager. En este momento, el denominador no es mónico, pero puede serlo. En esa línea, se modifica la fracción en el integrando para obtener

$$a(g_n) = \frac{1}{g_1 g_2 \cdots g_{n-2} g_{n-1}} \in F[g_n], \qquad b(g_n) = g_n \in F[g_n],$$

bajo la notación del teorema. Así, todos los supuestos de Rothstein-Trager se satisfacen, y es posible aplicarlo. El resultante correspondiente es

$$R(z) = \mathrm{res}_{g_n}\left(\frac{1}{g_1 g_2 \cdots g_{n-2} g_{n-1}} - \frac{z}{x g_1 g_2 \cdots g_{n-2} g_{n-1}}, g_n\right) = \frac{1}{g_1 g_2 \cdots g_{n-2} g_{n-1}}\left(1 - \frac{z}{x}\right).$$

Y es bastante claro que si $R(z) = 0$, entonces $z = x$, llegando a ceros no constantes. Esto es, las integrales de interés son no elementales para todo entero $n \geq 2$.

$\blacksquare$

Ejemplo 10.6: Potencias naturales de logaritmos.

A continuación, se demostrará que las integrales

$$\int [\log(x)]^n\,\mathrm{d}x$$

son elementales para todo $n \in \mathbb{N}$, y se dará la forma de la antiderivada.

Demostración. Nótese que la integral pertenece a la extensión $K(x, g)$, donde $g = \log(x)$. El polinomio logarítmico a integrar es $P(g) = g^n$, que claramente tiene grado n. Todos sus coeficientes son 0 a excepción del principal, que es 1. Luego, se tendrá el sistema

$$\begin{cases} 0 &= b_{n+1}', \\ 1 &= (n+1)g' b_{n+1} + q_n', \\ 0 &= n g' q_n + q_{n-1}', \\ & \vdots \\ 0 &= 2g' q_2 + q_1', \\ 0 &= g' q_1 + \overline{q_0}'. \end{cases}$$

Aquí, se debe cumplir que $q_k \in K(x)$, mientras que $\overline{q_0}$ sí puede pertencer a una extensión logarítmica de $K(x)$. La primera ecuación, como siempre, indica que b_{n+1} es constante. Como $g' = 1/x$, la segunda ecuación implica

$$q_n' = 1 - \frac{(n+1)b_{n+1}}{x}.$$

Ahora bien, esto es $q_n = x - (n+1)b_{n+1}\log(x) + b_n$, con b_n una constante. Sin embargo, $\log(x)$ no puede aparecer en $q_n \in K(x)$, por lo cual se debe tener que $b_{n+1} = 0$. Es decir, $q_n = x + b_n$. Ahora, en la tercera ecuación es fácil ver que se tendrá

$$0 = \frac{n(x+b_n)}{x} + q_{n-1}' \implies q_{n-1} = -nx + b_{n-1} + b_n \log(x) \implies q_{n-1} = -nx + b_{n-1}.$$

El argumento para hacer $b_n = 0$ es el mismo que en la anterior ecuación. En el siguiente caso,

$$0 = \frac{(n-1)(-nx + b_{n-1})}{x} + q_{n-2}' \implies q_{n-2} = n(n-1)x + b_{n-2}.$$

A partir de aquí, es posible observar inductivamente que

$$q_k = (-1)^{n-k}(n-k)!\binom{n}{n-k}x + b_k.$$

Además, también es claro que $b_k = 0$ para $1 \leq k \leq n+1$. Con esto, únicamente hace falta obtener $\overline{q_0}$. Nótese que es posible simplificar de manera que $q_1 = (-1)^{n-1}n!x$. Introduciendo esto a la última ecuación en el sistema,

$$0 = \frac{(-1)^{n-1}n!x}{x} + \overline{q_0}' \implies \overline{q_0} = (-1)^n n!x.$$

Con esto, el algoritmo encontró una antiderivada para $[\log(x)]^n$ en cualquier potencia natural $n \in \mathbb{N}$, de manera que dichas integrales son elementales y su forma general es:

$$\int [\log(x)]^n \, \mathrm{d}x = x \sum_{k=0}^{n} (-1)^{n-k}(n-k)!\binom{n}{n-k}(\log(x))^k.$$

■

Aplicada para n entre 1 y 4, esto se ve así:

$$\begin{aligned}
&\int \log(x)\, \mathrm{d}x = x(\log(x) - 1),\\
&\int [\log(x)]^2 \, \mathrm{d}x = x([\log(x)]^2 - 2\log(x) + 2),\\
&\int [\log(x)]^3 \, \mathrm{d}x = x([\log(x)]^3 - 3[\log(x)]^2 + 6\log(x) - 6),\\
&\int [\log(x)]^4 \, \mathrm{d}x = x([\log(x)]^4 - 4[\log(x)]^3 + 12[\log(x)]^2 - 24\log(x) + 24).
\end{aligned}$$

Así, observamos que el algoritmo de Risch puede ser útil para encontrar fórmulas generales interesantes, y no solo algunas integrales aisladas.

Ejemplo 10.7: Producto de logaritmos anidados.

Los productos en la forma $\log(x)\log(\log(x))\cdots\log(\log(\log(\cdots\log(x))))$ siempre poseen antiderivadas no elementales.

Demostración. Considérese una integral como la que se muestra a continuación:

$$\int \log(x)\log(\log(x))\,\mathrm{d}x\,.$$

Su integrando se encuentra en $K(x, g_1, g_2)$, donde $g_1 = \log(x)$ y $g_2 = \log(g_1)$. Se puede ver al integrando como $P(g_2) = g_1 g_2 \in K(x, g_1)[g_2]$. El sistema a resolver es, entonces,

$$\begin{cases} 0 = b_2', \\ g_1 = 2b_2 g_2' + q_1', \\ 0 = g_2' q_1 + \overline{q_0}'. \end{cases}$$

La primera ecuación nos dice que b_2 es constante. La segunda, se reescribe como

$$q_1' = \log(x) - \frac{2b_2}{x\log(x)} \implies q_1 = x\log(x) - x - 2b_2\log(\log(x)).$$

Sin embargo, como $q_1 \in K(x, g_1)$, es necesario que $b_2 = 0$ para que g_2 no aparezca en su expansión. Luego, $q_1 = x\log(x) - x$. Ahora, la tercera ecuación puede transformarse a

$$\overline{q_0}' = -1 + \frac{1}{\log(x)}.$$

Al integrar para obtener $\overline{q_0}$,

$$\overline{q_0} = -x + \int \frac{1}{\log(x)}\,\mathrm{d}x\,.$$

Puesto que el logaritmo integral aparece en su expansión, la integral es no elemental. Expresando la integral de cualquier manera, esta es

$$\int \log(x)\log(\log(x))\,\mathrm{d}x = (x\log(x) - x)\log(\log(x)) - x + \int \frac{1}{\log(x)}\,\mathrm{d}x\,.$$

De hecho, a partir de aquí, para demostrar que

$$\int \log(x)\log(\log(x))\cdots\underbrace{\log(\log(\log(\cdots\log(x))))}_{n\text{ logaritmos anidados.}}\,\mathrm{d}x$$

es no elemental, solo hace falta un proceso inductivo. En efecto, se demostró el caso base para $n = 2$ logaritmos. Supóngase que se cumple para n logaritmos que la integral es no elemental.

Considérese el caso de $n+1$ anidaciones. El integrando se encuentra en $K(x, g_1, g_2, \ldots, g_{n+1})$, donde $g_1 = \log(x)$ y $g_k = \log(g_{k-1})$. Visto como un polinomio, será $P(g_{n+1}) = (g_1 g_2 \cdots g_n)g_{n+1}$, miembro de $K(x, g_1, g_2, \ldots, g_n)[g_{n+1}]$. De esta manera, el sistema a satisfacer será

$$\begin{cases} 0 = b_2', \\ g_1 g_2 \cdots g_n = 2b_2 g_n' + q_1', \\ 0 = g_n' q_1 + \overline{q_0}'. \end{cases}$$

Se tendrá en primer lugar que b_2 será una constante, y que se cumple la ecuación

$$g_1 g_2 \cdots g_n = \frac{2b_2}{x g_1 g_2 \cdots g_n} + q_1'.$$

Esto directamente es imposible, pues se requeriría que

$$q_1 = -2b_2 g_{n+1} + \int g_1 g_2 \cdots g_n \, \mathrm{d}x \in K(x, g_1, g_2, \ldots, g_n).$$

Mientras que hacer $b_2 = 0$ solucionaría el problema de g_{n+1} apareciendo en la expansión de q_1, no hay manera de remover la integral al final de la misma. Esta integral es la que aparece en la hipótesis inductiva, por lo cual debe aparecer una integral no elemental en la expansión de q_1. Esto es, por el proceso de inducción, que las integrales con la forma mostrada son todas no elementales.

■

Ejemplo 10.8: Más generalizaciones en potencias.

En el ejemplo 10.4 se integraron expresiones del tipo $x^m[\log(x)]^n$, pero en el caso en el cual n era un entero negativo. Es decir, el logaritmo estaba en el denominador. Ahora, nos interesará

$$\int x^m [\log(x)]^n \, \mathrm{d}x \, ,$$

para cualquier m y para $n \in \mathbb{Z}^+$. Estas siempre son elementales.

Demostración. En este caso, se trabaja sobre $K(x, g)$, donde $g = \log(x)$. El polinomio a integrar es $P(g) = x^m g^n$. Considérese primero el caso en que $m = -1$. Entonces, del sistema de ecuaciones diferenciales se deberá cumplir que

$$\frac{1}{x} = \frac{(n+1)b_{n+1}}{x} + q_n',$$

para una constante b_{n+1} y para $q_n \in K(x)$. Pero esto es $q_n = (1 - (n+1)b_{n+1}) \log(x) + b_n$, por lo cual es necesario que $1 - (n+1)b_{n+1} = 0$. O bien,

$$b_{n+1} = \frac{1}{n+1}.$$

Desde luego, esto hace que $q_n = b_n$. La siguiente ecuación se convierte en $q_{n-1}' = nb_n/x$, lo cual es $q_{n-1} = nb_n \log(x)$, provocando que $b_n = 0$. Es claro que el patrón continúa, dado que todos los demás coeficientes de P son nulos, y entonces

$$\int \frac{[\log(x)]^n}{x} \, \mathrm{d}x = \frac{[\log(x)]^{n+1}}{n+1},$$

lo cual es fácil de comprobar por diferenciación directa.

Considérese ahora el caso en que $m \neq -1$. Lo único que cambia es la segunda ecuación en el sistema, la cual se convierte en

$$x^m = \frac{(n+1)b_{n+1}}{x} + q_n' \implies q_n = \frac{x^{m+1}}{m+1} - (n+1)b_{n+1} \log(x) + b_n.$$

Pero $q_n \in K(x)$, por lo cual $b_{n+1} = 0$. A continuación, se prosigue con las demás ecuaciones que están todas igualadas a cero.

$$q_{n-1}' = -\frac{nx^m}{m+1} - \frac{nb_n}{x} \implies q_{n-1} = -\frac{nx^{m+1}}{(m+1)^2} - nb_n \log(x) + b_{n-1}.$$

Aquí, se hace $b_n = 0$. Continuando,

$$q_{n-2}' = \frac{n(n-1)x^m}{(m+1)^2} - \frac{(n-1)b_{n-1}}{x} \implies q_{n-2} = \frac{n(n-1)x^{m+1}}{(m+1)^3} - (n-1)b_{n-1} \log(x) + b_{n-2}.$$

Y es claro que $b_{n-1} = 0$. En general, se llega inductivamente a que

$$q_k = (-1)^{n-k}(n-k)!\binom{n}{k}\frac{x^{m+1}}{(m+1)^{n-k+1}}.$$

Y, como en el ejemplo 10.6, con un poco de trabajo es posible mostrar que la función $\overline{q_0}$ presenta un comportamiento similar, de manera que puede incluirse entre las demás q_k. Al final de cuentas, la integral es elemental y puede expresarse a través de la expresión

$$\int x^m[\log(x)]^n \,\mathrm{d}x = x^{m+1}\sum_{k=0}^{n}(-1)^{n-k}(n-k)!\binom{n}{k}\frac{[\log(x)]^k}{(m+1)^{n-k+1}}.$$

Al final, complementando con el ejemplo 10.4, se concluye que las integrales de las funciones con la forma $x^m[\log(x)]^n$ son elementales para todo m cuando n es un entero no negativo, también son elementales cuando $m = -1$ en cualquier caso para n (incluyendo valores no enteros de n, pero esto requiere integración de funciones algebraicas), mientras que son no elementales para todo $m \neq -1$ cuando n es un entero negativo.

■

Ejemplo 10.9: Logaritmo de un polinomio.

La antiderivada del logaritmo de un polinomio siempre es elemental.

Demostración. Considérese el integrando $g = \log(p(x))$, donde $p(x) \in \mathbb{C}[x]$ es un polinomio. Entonces $g' = p'/p$, y el sistema estará dado por

$$\begin{cases} 0 = b_2', \\ 1 = 2b_2\frac{p'}{p} + q_1', \\ 0 = q_1\frac{p'}{p} + \overline{q_0}'. \end{cases}$$

Esto implica que b_2 es constante, y que $q_1 = x$. Así, se llega a que

$$\overline{q_0} = -\int \frac{xp'(x)}{p(x)}\,\mathrm{d}x\,.$$

Esta es una integral de una función racional, lo cual implica que $\int \log(p(x))\,\mathrm{d}x$ siempre es elemental:

$$\int \log(p(x))\,\mathrm{d}x = x\log(p(x)) - \int \frac{xp'(x)}{p(x)}\,\mathrm{d}x\,.$$

■

Nota Bene 10.2: Integral del seno inverso.

En la formalidad de la teoría que estamos trabajando, se esperaría que no estemos listos para integrar funciones como el seno inverso. Por la ecuación 14.3, esta es

$$\int \sin^{-1}(x)\,\mathrm{d}x = \int -i\log\left(\sqrt{1-x^2}+ix\right)\mathrm{d}x\,.$$

Esta función está en el campo diferencial $\mathbb{C}(x, \sqrt{1-x^2}, g)$, donde $g = -i\log\left(\sqrt{1-x^2}+ix\right)$, o equivalentemente, $g = \sin^{-1}(x)$. Nótese que la extensión $\sqrt{1-x^2}$ no es trascendental sobre $\mathbb{C}(x)$, por lo cual los teoremas que hemos demostrado no aplican. Sin embargo, g sí es una extensión logarítmica de $\mathbb{C}(x, \sqrt{1-x^2})$, pues cumple

$$g' = \frac{1}{\sqrt{1-x^2}}.$$

De esta manera, el integrando puede ser escrito como el polinomio $P(g) = g \in \mathbb{C}(x, \sqrt{1-x^2})[g]$. Suponiendo que el teorema 10.2 sí aplica, se obtiene el sistema de ecuaciones

$$\begin{cases} 0 = b_2', \\ 1 = \frac{2b_2}{\sqrt{1-x^2}} + q_1', \\ 0 = \frac{q_1}{\sqrt{1-x^2}} + \overline{q_0}'. \end{cases}$$

De la primera ecuación, se llega a que b_2 es constante. De la segunda, se tiene

$$q_1 = \int \left(1 - \frac{2b_2}{\sqrt{1-x^2}}\right) \mathrm{d}x = x - 2b_2 \sin^{-1}(x).$$

Pero $q_1 \in \mathbb{C}(x, \sqrt{1-x^2})$, por lo cual $b_2 = 0$ y $q_1 = x$. Introduciendo esto a la tercera ecuación, se obtiene directamente

$$\overline{q_0} = \int \frac{-x}{\sqrt{1-x^2}} \, \mathrm{d}x \,. \tag{10.9}$$

En este procedimiento, podría darse una segunda objeción: aún no sabemos integrar expresiones como la que aparece en $\overline{q_0}$. Al no tener mecanismos, se requiere de notar que si $\theta = \sqrt{1-x^2}$, entonces $\theta^2 = 1 - x^2$, de manera que $2\theta\theta' = -2x$, y por lo tanto

$$\left(\sqrt{1-x^2}\right)' = \frac{-x}{\sqrt{1-x^2}}.$$

Pero claro, esto no es más que una formalidad, pues esta integral es integrable por sustitución. Al final de cuentas, se tiene $\overline{q_0} = \sqrt{1-x^2}$, de lo cual se obtiene la integral final:

$$\int \sin^{-1}(x) \, \mathrm{d}x = x \sin^{-1}(x) + \sqrt{1-x^2}.$$

Y en efecto, esta es la respuesta esperada. Sin embargo, como se recalcó al inicio de este ejemplo, las hipótesis del teorema 10.2 no se cumplen al presentarse una función algebraica en el campo diferencial de trabajo. Y es que, desde el inicio del capítulo, se recalcó que el campo diferencial utilizado debe ser un campo de funciones elementales trascendentales. Pero si es así, ¿por qué funciona el teorema? Principalmente, la objeción sobre la falta de herramientas para integrar funciones como en la ecuación 10.9 es la culpable de este formalismo. El teorema de integración de polinomios logarítmicos puede ser extendido a campos de funciones elementales generales, pero si tomamos esta decisión, no siempre tendremos un algoritmo para integrar las funciones algebraicas que puedan aparecer. Esto es, de cualquier manera, un problema que puede arreglarse a través del estudio de algoritmos de integración simbólica de funciones algebraicas, haciendo uso de geometría algebraica.

10.2. Extensiones exponenciales trascendentales

Similar a la sección anterior, se tomará f como en la ecuación 10.1, pero esta vez g_N será una extensión exponencial sobre F_{N-1}. Esto es, existe $u \in F_{N-1}$ tal que $g_N' = u' g_N$, lo cual denotamos por $g_N = \exp(u)$.

Aunque se esperaría que los resultados fueran exactamente los mismos y las pruebas tuvieran cambios mínimos, será necesario modificar los teoremas de integración en extensiones exponenciales. Específicamente, la aplicación del algoritmo de Hermite requiere un poco más de trabajo previo, los teoremas de Rothstein-Trager requieren un supuesto y un término extra, y el teorema de integración de polinomios exponenciales cambia por completo al sistema de ecuaciones diferenciales. Sin embargo, la dificultad técnica no recibe muchos cambios. Por ahora, procedemos a generalizar los teoremas de integración de funciones racionales a una función racional en el símbolo exponencial g_N sobre el campo $K(x, g_1, \ldots, g_{N-1})$.

10.2.1. Aplicación del algoritmo de Hermite en extensiones exponenciales

A continuación, se aplicará el algoritmo de separación de la integral de Hermite para el caso de extensiones exponenciales. En esta aplicación, será necesario realizar modificaciones extras debido a las peculiaridades diferenciales de los exponenciales demostradas en el capítulo 7.

Realizando el algoritmo de la división, existen $P(g_N), r(g_N) \in F_{N-1}[g_N]$ tales que

$$f(g_N) = \frac{p(g_N)}{q(g_N)} = P(g_N) + \frac{r(g_N)}{q(g_N)},$$

donde $r(g_N) = 0$ o $\deg(r(g_N)) < \deg(q(g_N))$. De esta manera,

$$\int f(g_N) = \int P(g_N) + \int \frac{r(g_N)}{q(g_N)}.$$

A diferencia del caso logarítmico, estas integrales aún no son la parte polinómica y racional que nos interesan. Esto se debe a que la segunda no cumple aún con los supuestos de Hermite.

Hagamos el intento de aplicar el algoritmo de Hermite para la integral $\int \frac{r(g_N)}{q(g_N)}$. En primer lugar, se factora $q(g_N) = \prod_{k=1}^{n} q_k(g_N)^k$ donde cada $q_k(g_N)$ es mónico y libre de cuadrados, con $(q_i(g_N), q_j(g_N)) = 1$ para $i \neq j$, y $\deg(q_k(g_N)) > 0$. Aquí, que $q_k(g_N)$ sea libre de cuadrados es una propiedad en $F_{N-1}[g_N]$, por lo cual $\big(q_k(g_N), D_{g_N}[q_k(g_N)]\big) = 1$. A diferencia del caso logarítmico, no necesariamente es cumple que $\big(q_k(g_N), [q_k(g_N)]'\big) = 1$. Por ejemplo, si $q_k(g_N) = g_N$, entonces

$$\big(q_k(g_N), [q_k(g_N)]'\big) = (g_N, g_N') = (g_N, u' g_N) = g_N \neq 1.$$

Sin embargo, por el teorema 7.3, se conoce que $q_k(g_N) \mid [q_k(g_N)]'$ si y solo si $q_k(g_N)$ es un monomio. Esto hará cumplirse lo deseado, siempre que se eliminen los monomios del denominador.

Escríbase $q(g_N) = g_N^{\alpha} \bar{q}(g_N)$, donde $g_N \nmid \bar{q}(g_N)$, y $\bar{q}(g_N) \in F_{N-1}[g_N]$. De esta manera, α es el exponente más pequeño que hace que el coeficiente de g_N^{α} sea no nulo. Si se diera que $\alpha = 0$, entonces se cumple $\big(q_k(g_N), [q_k(g_N)]'\big) = 1$ y Hermite aplica. Si no, se realiza el procedimiento a continuación. Es posible encontrar $\bar{r}(g_N), w(g_N) \in F_{N-1}(g_N)$ tales que $\deg(\bar{r}(g_N)) < \deg(\bar{q}(g_N))$ y $\deg(w(g_N)) < \deg(g_N^{\alpha})$ que cumplan

$$\bar{r}(g_N) g_N^{\alpha} + w(g_N) \bar{q}(g_N) = r(g_N).$$

Dividiendo esta ecuación dentro de $q(g_N)$, y reemplazando la expresión obtenida en la expansión de $f(g_N)$, esto indica que

$$f(g_N) = P(g_N) + \frac{w(g_N)}{g_N^{\alpha}} + \frac{\bar{r}(g_N)}{\bar{q}(g_N)}.$$

Escribiendo $\bar{P}(g_N) = P(g_N) + \frac{w(g_N)}{g_N^{\alpha}}$, se tiene entonces a resolver

$$\int f(g_N) = \int \bar{P}(g_N) + \int \frac{\bar{r}(g_N)}{\bar{q}(g_N)}. \tag{10.10}$$

Mientras que $\bar{P}(g_N)$ no es un polinomio con potencias positivas en g_N, este puede verse como un polinomio extendido. Si $w(g_N) = \sum_{k=0}^{\alpha-1} w_k g_N^k$, entonces puede escribirse $w(g_N)/g_N^{\alpha} = \sum_{k=-\alpha}^{-1} w_{k+\alpha} g_N^k$. De esta manera,

$$\bar{P}(g_N) = \sum_{k=-\alpha}^{\lambda} \bar{P}_k g_N^k,$$

donde $\lambda = \deg(P(g_N))$ y $\bar{P}_k \in F_{N-1}$. La aparición de exponentes negativos podría causar preocupación, pero en realidad no aumentará la dificultad del cálculo de la parte polinomial de la integral, puesto que $g_N = \exp(u)$ implica que $g_N^{-k} = \exp(-ku)$.

Ahora sí, puede aplicarse el teorema de Hermite a la parte racional de la integral, esta vez interesando el integrando $\frac{\bar{r}(g_N)}{\bar{q}(g_N)}$. Primero, encuéntrese la factoración libre de cuadrados del nuevo denominador $\bar{q}(g_N) = \prod_{k=1}^{n} q_k(g_N)^k$, de manera que cada $q_k(g_N)$ sea mónico y libre de cuadrados, y $(q_i(g_N), q_j(g_N)) = 1$ para $i \neq j$. Además, $\deg(q_k(g_N)) > 0$ y $g_N \nmid q_k(g_N)$. Con esto, ya es posible demostrar la propiedad necesaria para culminar la aplicación del algoritmo de Hermite.

Propiedad 10.2: Sea F un campo diferencial con un símbolo x, donde el operador diferencial $' : F \to F$ es tal que $x' = 1$. Sea $F(g_N)$ una extensión diferencial de F con el mismo campo de constantes, siendo g_N exponencial y trascendental sobre F. Sea $a(g_N) \in F[g_N]$ mónico con grado positivo, libre de cuadrados en $F[g_N]$, y tal que $g_N \nmid a(g_N)$. Entonces, $\big(a(g_N), [a(g_N)]'\big) = 1$.

Demostración. Del teorema de derivadas de polinomios con entradas exponenciales, se sabe que $[a(g_N)]' \in F[g_N]$. Sea $F(\beta_1, \beta_2, \ldots, \beta_k)$ el campo de descomposición de $a(g_N)$, con lo cual

$$a(g_N) = \prod_{k=1}^{m} (g_N - \beta_k).$$

Entonces, diferenciando con respecto a x, y tomando $g_N' = u' g_N$ para $u \in F$, se tiene

$$[a(g_N)]' = \sum_{k=1}^{m} (u' g_N - \beta_k') \prod_{j \neq k} (g_N - \beta_j). \tag{10.11}$$

Aquí, dado que $a(g_N)$ es libre de cuadrados en $F[g_n]$, se debe cumplir que los β_k son distintos.

Desde luego, se cumplirá que $[a(g_N)]'$ tiene $m-1$ términos divisibles entre $g_N - \beta_k$ para cualquier k. Supóngase que existe algún k para el cual se cumpla que los m términos son divisibles, lo cual solo ocurriría si $g_N - \beta_k \mid u' g_N - \beta_k'$. Sea $v \in F_{N-1}$ tal que $u' g_N - \beta_k' = v(g_N - \beta_k)$. Entonces, igualando coeficientes, se requiere $u' = v$ y $-\beta_k' = -v\beta_k$. Juntando esto, se tiene que $\beta_k' = u'\beta_k$. Pero, como $g_N \nmid a(g_N)$, entonces $\beta_k \neq 0$, lo cual implicaría necesariamente que $\beta_k = \exp(u)$. Luego,

$$\left(\frac{g_N}{\beta_k}\right)' = \frac{\beta_k g_N' - \beta_k' g_N}{\beta_k^2} = \frac{\beta_k u' g_N - u' \beta_k g_N}{\beta_k^2} = 0.$$

Así, $g_N/\beta_k \in \operatorname{con}(F(g_N, \beta_1, \ldots, \beta_m))$. De manera análoga a la argumentación en la propiedad 10.1, esto implica que $C = g_N/\beta_k \in \operatorname{con}(F(\beta_1, \ldots, \beta_m))$. Pero entonces $g_N = C\beta_k \in \operatorname{con}(F(\beta_1, \ldots, \beta_m))$, lo cual contradice que g_N sea trascendental sobre F. Con esto, se imposibilita que $[a(g_N)]'$ comparta algún factor con $a(g_N)$, demostrando el resultado.

∎

Haciendo uso de esta herramienta, es posible realizar el algoritmo de Hermite exactamente como en el caso logarítmico, de manera que existe la representación

$$\int \frac{\bar{r}(g_N)}{\bar{q}(g_N)} = \frac{c(g_N)}{d(g_N)} + \int \frac{a(g_N)}{b(g_N)},$$

donde $\deg(a(g_N)) < \deg(b(g_N))$, siendo $b(g_N)$ mónico y libre de cuadrados, con $g_N \nmid b(g_N)$, y todos estos polinomios siendo parte de $F_{N-1}[g_N]$. Así, todo el trabajo restante en el caso racional es culminar con el proceso de Rothstein y Trager.

10.2.2. Rothstein-Trager en la extensión exponencial

Habiendo separado la integral en una pieza con los requerimientos de Rothstein-Trager, únicamente es necesario demostrar un teorema análogo que tome en cuenta las peculiaridades de la extensión exponencial sobre la cual se trabaja. En este caso, se presentan dos cambios importantes con respecto al caso logarítmico: el denominador del integrando no puede ser un monomio, y podrá aparecer un término no logarítmico en la representación de las integrales. Dicho término será un múltiplo constante del argumento de la exponencial en la última extensión.

Teorema 10.3 (Rothstein-Trager para funciones exponenciales)**:** Sea F un campo de funciones elementales y $K = \operatorname{con}(F)$. Sea g trascendental y exponencial sobre F, con $g = \exp(u)$ para $u \in F$. Supóngase también que la extensión elemental trascendental $F(g)$ tiene el mismo campo de constantes que F. Considérese $a(g), b(g) \in F[g]$ con $\big(a(g), b(g)\big) = 1$, con $\deg(a(g)) < \deg(b(g))$, y con $b(g)$ mónico y libre de cuadrados, tal que $g \nmid b(g)$. Defínase, adicionalmente,

$$R(z) = \operatorname{res}_g \big(a(g) - z[b(g)]', b(g)\big) \in F[z],$$

con raíces c_k para $1 \leq k \leq m$. Además, se definen

$$v_k(g) = \big(a(g) - c_k[b(g)]', b(g)\big) \in F(c_1, \ldots, c_m)[g],$$

de manera que se cumple:

- $\displaystyle\int \frac{a(g)}{b(g)}$ es elemental si y solo si las raíces de $R(z) \in F[z]$ son constantes no todas nulas.
- Si $\displaystyle\int \frac{a(g)}{b(g)}$ es elemental, luego $\displaystyle\frac{a(g)}{b(g)} = \gamma' + \sum_{k=1}^{m} c_k \frac{[v_k(g)]'}{v_k(g)}$ donde $\displaystyle\gamma = -\left(\sum_{k=1}^{m} c_k \deg(v_k(g))\right) u$.
  De esta manera,
  $$\int \frac{a(g)}{b(g)} = \gamma + \sum_{k=1}^{m} c_k \log(v_k(g)).$$
- Si F^* es la mínima extensión algebraica de F tal que se cumple el enunciado anterior, entonces debe darse que $F^* = F(c_1, c_2, \ldots, c_m)$.

Demostración. Supóngase que $\displaystyle\int \frac{a(g)}{b(g)}$ es elemental. Entonces, por el principio de Liouville

$$\frac{a(g)}{b(g)} = [v_0(g)]' + \sum_{k=1}^{m} c_k \frac{[v_k(g)]'}{v_k(g)},$$

donde $c_k \in K^*$ y $v_k(g) \in F^*(g)$, tomando K^* y F^* como las extensiones algebraicas mínimas de K y F que contengan a los c_k necesarios para expresar la integral. Como se hizo en el teorema de Rothstein-Trager para extensiones logarítmicas, es posible suponer que los c_k son distintos y no nulos, y que los $v_k(g)$ son polinomios en $F^*[g]$, libres de cuadrados, y primos relativos por pares.

En cuanto a $v_0(g)$, inicialmente no posee restricciones. Escríbase $v_0(g) = p_0(g)/q_0(g)$, para $p_0(g)$ y $q_0(g)$ polinomios primos relativos en $F^*[g]$. Si $q_0(g)$ contuviera un factor no monomial, entonces $[v_0(g)]'$ tendría en su denominador un factor sin libertad de cuadrados, el cual no podría cancelar sus factores cuadrados debido al tercer punto del teorema 7.3, y debido a que $p_0(g)$ y $q_0(g)$ son primos relativos. Por la forma general de la derivada de una función racional que se observa en la ecuación 9.4, esto no puede ocurrir, pues $b(g)$ es libre de cuadrados. Entonces, debe tenerse que $q_0(g) = hg^\nu$, donde $\nu \geq 0$ y $h \in F^*$. Con esto, si $\deg(p_0(g)) = \ell$, entonces

$$v_0(g) = \frac{p_0(g)}{hg^\nu} = \sum_{k=-\nu}^{\ell-\nu} h_k g^k,$$

con $h_k \in F^*$. De nuevo por el teorema de diferenciación de polinomios exponenciales, existen $\bar{h}_k \in F^*$ con las especificaciones de dicho teorema tales que

$$[v_0(g)]' = \sum_{k=-\nu}^{\ell-\nu} \bar{h}_k g^k.$$

Supóngase que $\ell - \nu > 0$. Como $\deg(v_k(g)) = \deg([v_k(g)]')$, y observando que

$$\frac{a(g)}{b(g)} = \sum_{k=-\nu}^{\ell-\nu} \bar{h}_k g^k + \sum_{k=1}^{m} c_k \frac{[v_k(g)]'}{v_k(g)},$$

entonces al obtener un denominador común para los términos en la derecha se tendría que multiplicar los $v_k(g)$ por los $\bar{h}_k g^k$ para los grados positivos, y esto resultaría en un numerador con grado mayor al denominador, lo cual contradice que $\deg(a(g)) < \deg(b(g))$. Entonces, como tampoco es posible que $\ell - \nu < 0$ por la misma condición sobre los grados de $a(g)$ y $b(g)$, se concluye que $\ell - \nu = 0$.

Ahora, si $\nu > 0$, entonces g aparece en el denominador de $[v_0(g)]'$, y como los $[v_k(g)]'/v_k(g)$ no poseen a g en su denominador, tomando denominadores comunes se llega a que $g \mid b(g)$. Esto no es posible por hipótesis, de manera que es necesario que $\nu = 0$. Pero entonces, $[v_0(g)]' = h_0' \in F^*$. A partir de aquí, se utilizan los mismos argumentos de Rothstein-Trager racional para llegar a que los $v_k(g)$ pueden tomarse mónicos, de manera que

$$b(g) = \prod_{k=1}^{m} v_k(g).$$

En consecuencia, es posible reescribir la expresión para $a(g)/b(g)$ como

$$\frac{a(g)}{\prod_{k=1}^{m} v_k(g)} = h_0' + \sum_{k=1}^{m} c_k \frac{[v_k(g)]'}{v_k(g)}. \tag{10.12}$$

Nótese que la fracción en la izquierda de esta ecuación es propia, pues el denominador tiene grado mayor al numerador, y no tienen factores comunes puesto que $(a(g), b(g)) = 1$.

En la derecha de la misma ecuación 10.12, se tiene que los grados en cada término de la sumatoria son iguales. Esto puede modificarse de manera que los términos en la derecha también representen una fracción propia. Escríbase $h_0 = \gamma + H$, donde γ es como definido en la hipótesis, y $H \in F^*$ existe al ser F^* un campo. Entonces,

$$\frac{a(g)}{\prod_{k=1}^{m} v_k(g)} = H' + \sum_{k=1}^{m} c_k \left(\frac{[v_k(g)]'}{v_k(g)} - \deg(v_k(g))u' \right).$$

Inspeccionése momentáneamente el interior de esta sumatoria. Tomando el denominador común, este puede escribirse como

$$\frac{a(g)}{\prod_{k=1}^{m} v_k(g)} = H' + \sum_{k=1}^{m} c_k \left(\frac{[v_k(g)]' - \deg(v_k(g))u'v_k(g)}{v_k(g)} \right). \tag{10.13}$$

Es posible mostrar que $[v_k(g)]'$ y $\deg(v_k(g))u'v_k(g)$ comparten el mismo coeficiente principal, provocando que el interior de dicha sumatoria sea una fracción propia. En el caso de $[v_k(g)]'$, puesto que $v_k(g)$ es mónico se tiene

$$[v_k(g)]' = \left(\sum_{j=0}^{\eta} V_j g^j \right)' = V_0' + \sum_{j=1}^{\eta} (V_j' + ju'V_j) g^j = V_0' + \sum_{j=1}^{\eta-1} (V_j' + ju'V_j) g^j + \eta u' g^\eta.$$

Mientras tanto, la expansión para $\deg(v_k(g))u'v_k(g)$ es

$$\deg(v_k(g))u'v_k(g) = \eta u' \left(\sum_{j=0}^{\eta} V_j g^j \right) = \eta u' \left(\sum_{j=0}^{\eta-1} V_j g^j \right) + \eta u' g^{\eta}.$$

Por lo tanto, al restar ambas expresiones, sus coeficientes principales se cancelan. Luego,

$$\deg\big([v_k(g)]' - \deg(v_k(g))u'v_k(g)\big) < \deg(v_k(g)). \tag{10.14}$$

De este modo, los términos dentro de la sumatoria en la ecuación 10.13 son fracciones propias, de manera que la sumatoria es en su totalidad una fracción propia al tomar el denominador común. Si $H' \neq 0$, entonces al tomar el denominador común con la sumatoria se tendría de nuevo una fracción impropia, pues se recuperaría que los grados del numerador y denominador son los mismos. Esto no es posible, lo cual implica que $H' = 0$. Como $h_0' = \gamma' + H'$, esto implica que la ecuación 10.12 puede reescribirse simplemente como

$$\frac{a(g)}{b(g)} = \gamma' + \sum_{k=1}^{m} c_k \frac{[v_k(g)]'}{v_k(g)}.$$

Aplicando el teorema de Rothstein-Trager en caso racional sobre $a(g)/b(g) - \gamma'$, los $c_k \in K^*$ son las raíces distintas de $R(z)$, y se obtiene $v_k(g) = \big(a(g) - c_k[b(g)]', b(g)\big) \in F(c_1, \ldots, c_m)[g]$ para cada k. Esto demuestra la implicación necesaria del primer punto, y demuestra a su vez el segundo y el tercer punto como se argumentó en el teorema 10.1.

Finalmente, supóngase que todas las raíces de $R(z)$ son constantes, sean $c_k \in K^*$ las raíces distintas de $R(z)$ y sean

$$v_k(g) = \big(a(g) - c_k[b(g)]', b(g)\big) \in F(c_1, \ldots, c_m)[g].$$

De nuevo, se argumenta como en la versión logarítmica para llegar a

$$b(g) = \prod_{k=1}^{m} v_k(g).$$

Además, los $v_k(g)$ son mónicos, primos relativos por pares. Ahora, defínase $\bar{a}(g) \in F[g]$ tal que

$$\bar{a}(g) = \gamma' b(g) + \sum_{k=1}^{m} c_k [v_k(g)]' \prod_{j \neq k}^{1 \leq j \leq m} v_j(g), \tag{10.15}$$

donde γ es como se definió inicialmente. Es claro que $[b(g)]' = \sum_{k=1}^{m} [v_k(g)]' \prod_{j \neq k}^{1 \leq j \leq m} v_k(g)$, por lo cual se tendrá

$$\bar{a}(g) - c_i[b(g)]' = \gamma' b(g) + \sum_{k=1}^{m} (c_k - c_i)[v_k(g)]' \prod_{j \neq k}^{1 \leq j \leq m} v_j(g).$$

De aquí, es claro que $v_i(g) \mid \bar{a}(g) - c_i[b(g)]'$ para cada índice i, al igual que por definición se tiene $v_i(g) \mid a(g) - c_i[b(g)]'$ para cada índice i. Restando las divisibilidades, se tiene que $v_i(g) \mid \bar{a}(g) - a(g)$. Por la independencia en factores entre los $v_i(g)$, dado que $b(g)$ es el producto entre ellos se tiene

$$b(g) \mid \bar{a}(g) - a(g). \tag{10.16}$$

Sin embargo, debido a la definición de γ y debido a que $b(g) = \prod_{k=1}^{m} v_k(g)$, la ecuación 10.15 puede representarse como

$$\begin{aligned} \bar{a}(g) &= -\left(\sum_{k=1}^{m} c_k \deg(v_k(g)) \right) \prod_{k=1}^{m} v_k(g) + \sum_{k=1}^{m} c_k [v_k(g)]' \prod_{j \neq k}^{1 \leq j \leq m} v_j(g) \\ &= \sum_{k=1}^{m} c_k \prod_{j \neq k}^{1 \leq j \leq m} v_j(g)\big([v_k(g)]' - \deg(v_k(g))u'v_k(g)\big). \end{aligned}$$

Pero por la relación 10.14, se tiene que el grado de cada factor $[v_k(g)]' - \deg(v_k(g))u'v_k(g)$ es menor al grado de $v_k(g)$. Como $b(g) = \prod_{k=1}^{m} v_k(g)$, esto implica entonces que $\deg(\bar{a}(g)) < \deg(b(g))$. Pero como $\deg(a(g)) < \deg(b(g))$, se tiene entonces que $\deg(\bar{a}(g) - a(g)) < \deg(b(g))$. Esto implica que necesariamente $\bar{a}(g) - a(g) = 0$, debido al resultado en la relación 10.16. Pero entonces,

$$\frac{a(g)}{b(g)} = \frac{\gamma' b(g) + \sum_{k=1}^{m} c_k [v_k(g)]' \prod_{j\neq k}^{1\leq j\leq m} v_j(g)}{b(g)} = \gamma' + \sum_{k=1}^{m} c_k \frac{[v_k(g)]'}{v_k(g)}.$$

En otras palabras, se demostró por completo el resultado:

$$\int \frac{a(g)}{b(g)} = \gamma + \sum_{k=1}^{m} c_k \log(v_k(g)).$$

■

Habiendo demostrado este teorema, tenemos un mecanismo para determinar la integrabilidad de muchos tipos de funciones, pertenecientes a un campo de funciones elementales trascendentales cuya última extensión sea exponencial. A continuación, observamos algunos ejemplos.

Ejemplo 10.10: Exponencial desplazada por una constante.

Considérense las integrales del tipo

$$\int \frac{x^n}{\alpha + e^{\beta x}} \, \mathrm{d}x \,,$$

donde $e^{\beta x} = \exp(\beta x)$. Tomemos $g = e^{\beta x}$, de manera que el integrando pertenece a $K(x, g)$. Entonces, se tiene $a(g) = x^n$ y $b(g) = \alpha + g$, y luego $[b(g)]' = \beta g$. Con esto,

$$R(z) = \operatorname{res}_g (x^n - \beta z g, \alpha + g) = \det \begin{bmatrix} -\beta z & x^n \\ 1 & \alpha \end{bmatrix} = -\alpha\beta z - x^n.$$

Claramente, el cero de $R(z)$ tiene la forma $z = -x^n/\alpha\beta$. Por lo tanto, la integral es no elemental siempre que $n \neq 0$.

En caso que $n = 0$, se tendrá $z = -1/\alpha\beta$, y puede calcularse salvo asociación:

$$v(g) = \left(1 + \frac{g}{\alpha}, g + \alpha\right) = g + \alpha.$$

Haría falta calcular γ. Se tiene que $u = \beta x$. Además, únicamente se tiene al cero $c_1 = -1/\alpha\beta$, y $v(g)$ es de grado 1. Por lo tanto, el término adicional estará dado por $\gamma = x/\alpha$. Con esto,

$$\int \frac{1}{\alpha + e^{\beta x}} \, \mathrm{d}x = \frac{1}{\alpha\beta} \left[\beta x - \log\!\left(\alpha + e^{\beta x}\right)\right].$$

Ejemplo 10.11: Se considera una generalización de la integral del ejemplo anterior:

$$\int \frac{p(x)}{q(x) + e^{\beta x}} \, \mathrm{d}x \,.$$

Aquí, $p(x)$ y $q(x)$ son polinomios en $\mathbb{C}[x]$, y β es una constante. Tomamos $g = \exp(\beta x)$ de manera que la integral se presenta en el campo diferencial $\mathbb{C}(x, g)$. Según la notación de Rothstein-Trager, $a(g) = p(x)$ y $b(g) = q(x) + g$. Además $[b(g)]' = q'(x) + \beta g$, y así,

$$R(z) = \operatorname{res}_g \left(p(x) - z[q'(x) + \beta g], q(x) + g\right) = \det \begin{bmatrix} -\beta z & p(x) - zq'(x) \\ 1 & q(x) \end{bmatrix}.$$

Este determinante resulta en $R(z) = -\beta q(x)z + q'(x)z - p(x)$. Igualando a cero, se obtiene

$$z = \frac{p(x)}{q'(x) - \beta q(x)}.$$

Por lo tanto, la integral será elemental solo cuando $p(x)$ sea un múltiplo constante de $q'(x) - \beta q(x)$. Por simplicidad tomemos el caso $z = 1$. Entonces, por asociación,

$$v(g) = \big(-\beta q(x) - \beta g, q(x) + g\big) = q(x) + g.$$

Finalmente, puesto que $v(g)$ es lineal en g, que $u = \beta x$, y que $z = 1$, se tiene $\gamma = -\beta x$. Finalmente,

$$\int \frac{q'(x) - \beta q(x)}{q(x) + e^{\beta x}}\,\mathrm{d}x = \log\big(q(x) + e^{\beta x}\big) - \beta x.$$

Para el caso $z = \alpha \in \mathbb{C}$, simplemente se multiplica esta expresión por α en ambos lados.

Como puede observarse, la nueva restricción sobre los teoremas de Rothstein-Trager para extensiones exponenciales provoca que menos funciones sean antidiferenciables mediante esta vía. Casi cualquier función que en su denominador posea factores monomiales exponenciales se traslada al caso polinómico, aprovechando que los polinomios exponenciales contienen en ellos potencias negativas. Para finalizar, procedemos a mostrar este caso.

10.2.3. Sobre la integración de la pieza polinomial exponencial

Debido a los argumentos presentados al inicio de esta sección, la integración de la parte polinomial del caso exponencial concierne a un polinomio $\bar{P}(g_N)$ que posee potencias negativas de g_N:

$$\bar{P}(g_N) = \sum_{k=-\alpha}^{\lambda} \bar{P}_k g_N^k.$$

Seguidamente, se demostrará un teorema que da las condiciones necesarias para que $\int \bar{P}(g_N)$ sea elemental. Este es similar al teorema 10.2, pero contiene cambios bastante importantes que provocan dificultades nuevas en el caso de integración exponencial.

Teorema 10.4: Sea F un campo de funciones elementales y $K = \mathrm{con}(F)$. Sea g trascendental y exponencial sobre F, con $g = \exp(u)$ para $u \in F$. Supóngase también que la extensión elemental trascendental $F(g)$ tiene el mismo campo de constantes que F. Sea $\bar{P}(g) = \sum_{k=-\alpha}^{\lambda} \bar{P}_k g^k$, donde $\bar{P}_k \in F$. Sea además $\overline{K}$ la cerradura algebraica de K, y $\overline{F}$ la extensión de F tal que $\mathrm{con}(\overline{F}) = \overline{K}$. Si $\int \bar{P}(g)$ es elemental, entonces existen funciones $q_k \in \overline{F}$ para $k \neq 0$ y una función $\overline{q_0}$ en una extensión logarítmica de $\overline{F}$ tales que

$$\int \bar{P}(g) = \overline{q_0} + \sum_{k\neq 0}^{-\alpha\leq k\leq\lambda} q_k g^k,$$

las cuales satisfacen el sistema ecuaciones diferenciales:

$$\begin{cases} \bar{P}_0 = \overline{q_0}', \\ \bar{P}_k = q_k' + ku'q_k, \quad k \neq 0. \end{cases}$$

Cada ecuación en dicho sistema es independiente, en el sentido de que todas dependen únicamente de una función variable q_k o $\overline{q_0}$. A las ecuaciones diferenciales satisfechas por los q_k se les llama *ecuaciones diferenciales de Risch.*

Demostración. Si $\bar{P}(g)$ posee una antiderivada elemental, entonces se tiene por Liouville

$$\bar{P}(g) = [v_0(g)]' + \sum_{k=1}^{m} c_k \frac{[v_k(g)]'}{v_k(g)},$$

donde $c_k \in \overline{K}$ y $v_k(g) \in \overline{F}(g)$. Asumimos sin pérdida de generalidad que debe cumplirse una de dos: $v_k(g)$ no depende de g, o $v_k(g)$ es mónico e irreducible en $\overline{F}(g)$. Además, el elemento $v_0(g)$ no puede poseer factores no-monomiales en el denominador, como se vio anteriormente en la sección, y lo mismo es cierto sobre los factores de los $v_k(g)$. Esto implicaría que, si se diera el caso en que $v_k(g)$ depende de g, entonces $v_k(g) = g$ es la única posibilidad mónica, irreducible y monomial en $\overline{F}(g)$. Pero esto nos llevaría a que

$$c_k \frac{[v_k(g)]'}{v_k(g)} = c_k \frac{g'}{g} = c_k \frac{u' \exp(u)}{\exp(u)} = c_k u'.$$

Integrando esta expresión se obtendría $c_k \log(v_k(g)) = c_k u \in \overline{F}$, de manera que el logaritmo no es trascendental sobre F, y debería aparecer en la expansión de $v_0(g)$. Es entonces necesario que todos los $v_k(g)$ sean independientes de g, y los consideramos entonces como elementos $v_k \in \overline{F}$. Por otro lado, por las condiciones a las cuales está sujeto $v_0(g)$, este puede escribirse como un polinomio con potencias negativas en g. Así, reescribimos $\bar{P}(g)$ a través de

$$\bar{P}(g) = \left[\sum_{k=-\alpha}^{\lambda} q_k g^k \right]' + \sum_{k=1}^{m} c_k \frac{v_k'}{v_k}, \tag{10.17}$$

donde $q_k \in \overline{F}$ para cada k, y el rango de los índices k es el mismo de $\bar{P}(g)$ debido al teorema de difenciación de polinomios exponenciales. Diferenciando término por término, y reescribiendo $\bar{P}(g)$ a través de su sumatoria, esto implica que

$$\sum_{k=-\alpha}^{\lambda} \bar{P}_k g^k = \sum_{k=-\alpha}^{\lambda} (q_k' + k u' q_k) g^k + \sum_{k=1}^{m} c_k \frac{v_k'}{v_k}.$$

Igualando coeficiente por coeficiente, y escribiendo $\overline{q_0}' = q_0' + \sum_{k=1}^{m} c_k \frac{v_k'}{v_k}$, se obtiene el sistema:

$$\begin{cases} \bar{P}_0 = \overline{q_0}', \\ \bar{P}_k = q_k' + k u' q_k, \quad k \neq 0. \end{cases}$$

En efecto, por la construcción es claro que las soluciones están dadas por $q_k \in \overline{F}$ para cada índice $k \neq 0$, y por $\overline{q_0} \in \overline{F}(\log(v_1), \dots, \log(v_m))$ en el caso nulo. Reemplazando $\overline{q_0}$ e integrando en la ecuación 10.17 se tiene

$$\int \bar{P}(g) = \overline{q_0} + \sum_{k \neq 0}^{-\alpha \leq k \leq \lambda} q_k g^k.$$

■

Al igual que el teorema 10.2, lo demostrado aquí es útil para encontrar antiderivadas en el caso que estas existan, pero también puede utilizarse para demostrar que una antiderivada no existe. Sin embargo, en ambos casos, la tarea es más difícil. En el primero, porque la solución de la integral se traslada a solucionar una ecuación diferencial. En el segundo, porque no existe un algoritmo recursivo para solucionar este sistema debido a la independencia entre las ecuaciones diferenciales en el mismo. De hecho, para demostrar la inexistencia de una antiderivada elemental se deberá demostrar que una ecuación diferencial no posee solución en un campo diferencial específico. Aunque esto da una vía de solución, no siempre es tan inmediato como en el caso logarítmico. Procedemos con algunos ejemplos de aplicación del teorema 10.4.

Ejemplo 10.12: La función error.

La función error, mostrada a continuación, no posee una antiderivada elemental:

$$\operatorname{erf}(z) = \frac{2}{\sqrt{\pi}} \int_0^z e^{-x^2}\, \mathrm{d}x\,.$$

Demostración. Considérese el integrando $\exp\bigl(kx^2\bigr)$, donde $k \in \mathbb{C} - \{0\}$. Escríbase $g = \exp\bigl(kx^2\bigr)$, de manera que el integrando se encuentra en $\mathbb{C}(x, g)$. Nótese que este es un polinomio exponencial, dado por $P(g) = g$. Por el teorema 10.4, se tiene que si la integral es elemental entonces $\int g = q_1 g$, donde $q_1 \in \mathbb{C}(x)$ es solución de la ecuación diferencial de Risch

$$q_1' + 2kxq_1 = 1.$$

Tomemos $q_1(x) = a(x)/b(x)$ con $(a, b) = 1$, suponiendo que $\deg(b) \geq 1$. Luego,

$$\frac{ba' - b'a + 2kxab}{b^2} = 1.$$

Pero $\deg(b^2) > \deg(b) > \deg(b')$, y como $(a, b) = 1$, es imposible anular por completo a b^2 en la división. Esto no tendría sentido, debido a que el lado derecho de la ecuación es 1. Por lo tanto, se requiere que $\deg(b) = 0$. Tomamos entonces $q_1(x) \in \mathbb{C}[x]$.

Escríbase $\deg(q_1) = n$, de manera que $\deg(2kxq_1) = n+1$. Pero $\deg(q_1') \leq n$, y por lo tanto se tiene $\deg(q_1' + 2kxq_1) = n + 1$. Sin embargo, la ecuación $q_1' + 2kxq_1 = 1$ implicaría que $0 = \deg(1) = n + 1$. Esto nos llevaría a $\deg(q_1) = -1$, lo cual es absurdo. Por lo tanto, $\int \exp\bigl(kx^2\bigr)\, \mathrm{d}x$ es no elemental.

∎

Las demostraciones de que $\sin\bigl(kx^2\bigr)$ y $\cos\bigl(kx^2\bigr)$ no poseen antiderivadas elementales son prácticamente equivalentes utilizando las expresiones en el Anexo 14.1 para seno y coseno en términos de funciones exponenciales complejas.

Ejemplo 10.13: La función exponencial integral.

La función exponencial integral, mostrada a continuación, es no elemental:

$$\operatorname{Ei}(x) = \int_{-\infty}^{x} \frac{e^x}{x}\, \mathrm{d}x\,.$$

Demostración. Considérese el integrando $g = \frac{e^x}{x}$. Es claro que $g \in \mathbb{C}(x, e^x)$, y puede tomarse como un polinomio $P(g) = \frac{1}{x} g \in \mathbb{C}(x)[g]$. Si $\int P(g)$ es elemental, entonces existe $q_1 \in \mathbb{C}(x)$ tal que

$$q_1' + q_1 = \frac{1}{x}.$$

Sea $q_1(x) = p(x)/q(x)$ para $p, q \in \mathbb{C}[x]$ con $(p, q) = 1$. Por argumentos similares a los del teorema 6.1, se llega a que $x \mid q$, y se define $q = tx^n$ para $t \in \mathbb{C}[x]$ con $n \in \mathbb{Z}^+$, tal que $(t, x) = 1$. Además, se llega a que

$$pt(x - n) = x[t^2 x^{n-1} - p't + pt'],$$

lo cual implica que $x \mid pt(x - n)$. Pero $x \nmid t$ y $x \nmid x - n$, de lo cual $x \mid p$. Esto implica que $(p, q) \neq 1$, lo cual es un absurdo. Por lo tanto, no existe tal q_1, de manera que $\int \frac{e^x}{x}\, \mathrm{d}x$ es no elemental.

∎

Similar al caso de la función error, las demostraciones de que $\operatorname{Si}(x) = \frac{\sin(x)}{x}$ y $\operatorname{Ci}(x) = \frac{\cos(x)}{x}$ no tienen antiderivadas elementales usan casi exactamente el mismo argumento.

Ejemplo 10.14: La función x^x.

La siguiente integral no es expresable en términos de funciones elementales:

$$\int x^x \, \mathrm{d}x \, .$$

Demostración. Considérese el integrando $g = x^x$ el cual puede ser reescrito como $g = \exp(x \log(x))$. Nótese que

$$g' = (1 + \log(x)) \exp(x \log(x)) = (1 + \log(x))g.$$

Luego, se escoge el campo diferencial $K(x, \log(x), g)$, pues g es una extensión exponencial sobre $K(x, \log(x))$. Tomando $P(g) = g$ como un polinomio en $K(x, \log(x))[g]$, entonces si $P(g)$ posee antiderivada elemental, debe existir $q_1 \in K(x, \log(x))$ tal que

$$q_1' + (1 + \log(x))q_1 = 1.$$

Pero $\log(x)$ es trascendental sobre $K(x)$, por lo cual pueden igualarse coeficientes en la ecuación como polinomios en $K(x)[\log(x)]$. Esto puede escribirse como $q_1' + q_1 = 1$ para el grado 0 sobre $\log(x)$, y $q_1 = 0$ para el grado 1 sobre $\log(x)$. Esto implicaría que $1 = 0$, lo cual es absurdo. Por lo tanto, $\int x^x \, \mathrm{d}x$ es no elemental.

■

Los ejemplos aquí mostrados aprovechan el teorema 10.4 para demostrar que ciertas antiderivadas son no elementales. En caso que se desee utilizar dicho teorema para expresar la antiderivada elemental de una función, es necesario resolver las ecuaciones diferenciales de Risch. Es posible lograr esto de manera algorítmica en algunos casos, y puede encontrarse la teoría detrás de dichos algoritmos en el trabajo de Rothstein [21], Bronstein [3], y Davenport [7].

Los procedimientos mostrados a lo largo de este capítulo resuelven casi por completo el problema de antidiferenciación de funciones elementales trascendentales, con posibles problemas persistentes relacionados al aumento en la complejidad de un integrando. Sin embargo, el problema de la integración simbólica para funciones elementales que se encuentran en campos con adjunciones algebraicas requiere de aún más trabajo. La nota 10.2 en la sección sobre integración logarítmica demuestra que, aunque el álgebra para demostrar los teoremas de integración simbólica dentro de campos con extensiones algebraicas sea distinta y requiera herramientas más avanzadas, sus aplicaciones podrían resultar teniendo varias similitudes con respecto al trabajo hecho en las extensiones puramente trascendentales. Reiterando lo discutido al inicio de este capítulo, se invita al lector a visitar la literatura pertinente a la integración de funciones elementales algebraicas si desea conocer la última pieza del rompecabezas que es el algoritmo de integración de Risch.

CAPÍTULO 11

Conclusiones

- Se presentó una formalización matemática de la rama del Álgebra Diferencial, profundizando especialmente en la Integración Simbólica. Esto nos llevó a la determinación de integrabilidad de funciones, en ocasiones mezclando el problema con el mundo de la solución de ecuaciones diferenciales de primer orden.
- A lo largo de este trabajo se definió formalmente a las funciones elementales como objetos algebraicos, y se ahondó en las propiedades diferenciales que dichos objetos presentan. También se presentaron los campos de funciones elementales, dentro de los cuales se estableció una estructura especial.
- Se expusieron varios algoritmos de integración en términos finitos usando como base la integración de funciones racionales. El algoritmo de Rothstein-Trager presentó una mejora por encima de la descomposición por fracciones parciales de un denominador en sus factores lineales.
- Se demostraron varios teoremas que son utilizados ampliamente en la determinación de existencia de antiderivadas elementales. Como herramienta base se demostró el principio de Liouville, que presenta las condiciones necesarias para que la antiderivada de una función elemental sea también una función elemental.
- Se logró construir un algoritmo de integración que construye por completo la antiderivada de una función elemental trascendental, una vez demostrado que dicha antiderivada también sea elemental. Este algoritmo se basa en la aplicación del algoritmo de la división para separar a la integral en una parte *polinomial* y una parte *racional*, las cuales poseen teoremas específicos para su solución correspondiente. Este algoritmo fue aplicado para mostrar la inexistencia de representaciones en términos de funciones elementales para varias funciones especiales, como las famosas

$$\operatorname{erf}(z) = \frac{2}{\sqrt{\pi}} \int_0^z e^{-t^2}\,\mathrm{d}t\,, \qquad \operatorname{li}(x) = \int_0^x \frac{1}{\log(t)}\,\mathrm{d}t\,, \qquad \operatorname{Ei}(x) = \int_{-\infty}^x \frac{e^t}{t}\,\mathrm{d}t\,.$$

CAPÍTULO 12

Recomendaciones

- Resultaría conveniente ahondar en la Teoría Diferencial de Galois, que entre sus aplicaciones incluye la capacidad de determinar si las soluciones de ecuaciones diferenciales de mayor orden pueden ser expresadas en términos de funciones elementales, haciendo uso de la herramienta algebraica desarrollada por Galois en el siglo XIX.
- La definición presentada para funciones elementales provoca la necesidad de utilizar números complejos para resolver problemas que a menudo se encuentran dentro del campo real. Una recomendación para futuros investigadores es indagar en las funciones elementales reales, para desarrollar un algoritmo similar al mostrado, sin necesidad de adjuntar números complejos.
- Existen mejoras al algoritmo de Rothstein-Trager para la integración de funciones racionales, incluyendo el algoritmo de Lazard-Rioboo-Trager que minimiza la cantidad de ciclos a realizarse. Para la implementación óptima del algoritmo, existe un interés computacional en ampliar la investigación de esta u otras mejoras del mismo.
- Una posible adición al principio de Liouville se encuentra en la representación de antiderivadas no elementales, haciendo uso de funciones especiales como el logaritmo integral, la función error o los dilogaritmos como posibles nuevas piezas simples en la solución. También podría modificarse dicho principio haciendo uso de las funciones elementales reales.
- La aplicación de los teoremas de integración de polinomios logarítmicos y exponenciales resulta ser compleja en relación a los teoremas de Rothstein-Trager, sobre todo en el caso exponencial. Esto se debe a la aparición de sistemas de ecuaciones diferenciales, para las cuales debe demostrarse la existencia o inexistencia de una solución dentro de cierto campo de funciones elementales. Un desarrollo importante en la teoría podría presentarse en la recopilación de métodos sistemáticos de solución de estas ecuaciones diferenciales, de manera que la aplicación de dichos teoremas se simplifique significativamente.

CAPÍTULO 13

Bibliografía

[1] Ahlfors, Lars: *Complex Analysis.* International Series in Pure and Applied Mathematics, 1979.

[2] Baddoura, Jamil: *Integration in finite terms with elementary functions and dilogarithms.* Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, United States, 2006.

[3] Bronstein, Manuel: *The Transcendental Risch Differential Equation.* J. Symbolic Computation, 1988.

[4] Bronstein, Manuel: *A Unification of Liouvillian Extensions.* Applicable Algebra in Engineering Communication and Computing, 1990.

[5] Cherry, G. W. y B. F. Caviness: *Integration in Finite Terms with Special Functions: A Progress Report.* EUROSAM 84, 1984.

[6] Conway, J. B.: *Functions of one Complex Variable 1.* Springer, 1978.

[7] Davenport, J. H.: *The Risch Differential Equation Problem.* SIAM Journal on Computing, 1986.

[8] Geddes, K. O., S. R. Czapor y G. Labahn: *Algorithms for Computer Algebra.* Kluwer Academic Publishers, 1992.

[9] Hardy, G. H.: *The Integration of Functions of a Single Variable (Reprint).* Cambridge University Press, 1966.

[10] Hebisch, Waldemar: *Integration in terms of polylogarithm.* Wroclaw University, 2019.

[11] Hermite, M.: *Sur l'integration des Fractions Rationelles.* Nouvelles Annales de Mathematiques, 1872.

[12] Herstein, I. N.: *Topics in Algebra.* Blaisdell Publishing Company, 1964.

[13] Horowitz, E.: *Algorithms for Partial Fraction Decomposition and Rational Integration.* SYMSAC 71: Proceedings of the second ACM symposium on Symbolic and algebraic manipulation, 1971.

[14] Lazard, D. y R. Rioboo: *Integration of Rational Functions: Rational Computation of the Logarithmic Part*. J. Symbolic Comp., 1990.

[15] Liouville, Joseph: *Sur la détermination des intégrales dont la valeur est algébrique*. Journal de l'École polytechnique, 1833.

[16] Mack, D.: *On Rational Function Integration*. UCP-38, 1975.

[17] Masser, D. y U. Zannier: *Torsion points, Pell's equation, and integration in elementary terms*. Acta Mathematica, 2020.

[18] Risch, Robert H.: *The problem of integration in finite terms*. Transactions of the American Mathematical Society, 1969.

[19] Ritt, J. F.: *Integration in finite terms: Liouville theory of elementary methods*. Columbia University Press, 1948.

[20] Rosenlicht, Maxwell: *Integration in finite terms*. The American Mathematical Monthly, Vol. 79, No. 9, 1972.

[21] Rothstein, M.: *Aspects of Symbolic Integration and Simplification of Exponential and Primitive Functions*. Ph.D. Thesis, 1976.

[22] Trager, B. M.: *Algebraic Factoring and Rational Function Integration*. SYMSAC '76: Proceedings of the third ACM symposium on Symbolic and algebraic computation, 1976.

CAPÍTULO 14

Anexos

14.1. Expresiones para funciones elementales conocidas

En el capítulo 7, se definió formalmente a las funciones elementales a través del uso de las funciones logarítmicas, exponenciales y algebraicas como elementos de extensión para campos de funciones racionales. En dicha clasificación de funciones parecen hacer falta algunas funciones muy importantes en el cálculo. Por ejemplo, la ausencia de las funciones trigonométricas y sus inversos podría crear alerta. Sin embargo, en este anexo se muestra que dichas funciones sí están presentes, pues son combinaciones de funciones elementales sobre el campo de los números complejos.

14.1.1. Funciones trigonométricas

Del Análisis de Variable Compleja, se sabe que $e^{ix} = \cos(x) + i\sin(x)$. De aquí, se obtiene

$$\sin(x) = \frac{e^{ix} - e^{-ix}}{2i}, \qquad \cos(x) = \frac{e^{ix} + e^{-ix}}{2}. \tag{14.1}$$

Luego, también es claro que

$$\tan(x) = \frac{e^{ix} - e^{-ix}}{i(e^{ix} + e^{-ix})}. \tag{14.2}$$

En cuanto a las expresiones para $\csc(x)$, $\sec(x)$ y $\cot(x)$, simplemente es necesario calcular el recíproco multiplicativo de $\sin(x)$, $\cos(x)$ y $\tan(x)$, respectivamente.

14.1.2. Funciones trigonométricas inversas

De la ecuación 14.1, es posible demostrar que

$$\sin^{-1}(x) = -i\log\Big(\sqrt{1-x^2} + ix\Big). \tag{14.3}$$

Además, de la ecuación 14.2 se obtiene la expresión

$$\tan^{-1}(x) = \frac{i}{2}\big(\log(1-ix) - \log(1+ix)\big) = \frac{i}{2}\log\left(\frac{1-ix}{1+ix}\right). \tag{14.4}$$

Para obtener las cuatro funciones trigonométricas inversas restantes, es necesario utilizar las propiedades de reciprocidad y de complementos de ángulos. De esta manera,

$$\csc^{-1}(x) = \sin^{-1}\left(\frac{1}{x}\right), \qquad \cot^{-1}(x) = \tan^{-1}\left(\frac{1}{x}\right), \tag{14.5}$$

$$\cos^{-1}(x) = \frac{\pi}{2} - \sin^{-1}(x), \qquad \sec^{-1}(x) = \frac{\pi}{2} - \csc^{-1}(x). \tag{14.6}$$

Así, todas las funciones trigonométricas y sus inversas pueden ser expresadas a través de funciones elementales sobre el campo $\mathbb{C}$.

14.1.3. Funciones hiperbólicas y sus inversas

Es claro que las funciones hiperbólicas $\sinh(x)$, $\cosh(x)$, $\tanh(x)$, y sus recíprocos, son elementales al ser combinaciones de campo de exponenciales:

$$\sinh(x) = \frac{e^x - e^{-x}}{2}, \qquad \cosh(x) = \frac{e^x + e^{-x}}{2}, \qquad \tanh(x) = \frac{\sinh(x)}{\cosh(x)}. \tag{14.7}$$

Además, también es posible calcular sus inversos a través de las siguientes representaciones:

$$\sinh^{-1}(x) = \log\Big(\sqrt{1+x^2} + x\Big), \qquad \cosh^{-1}(x) = \log\Big(\sqrt{1-x^2} + x\Big), \tag{14.8}$$

$$\tanh^{-1}(x) = \frac{1}{2}\log\left(\frac{1+x}{1-x}\right), \qquad \coth^{-1}(x) = \tanh^{-1}\left(\frac{1}{x}\right), \tag{14.9}$$

$$\operatorname{sech}^{-1}(x) = \cosh^{-1}\left(\frac{1}{x}\right), \qquad \operatorname{csch}^{-1}(x) = \sinh^{-1}\left(\frac{1}{x}\right). \tag{14.10}$$

Todas estas relaciones se desprenden de simple álgebra de funciones inversas. De esta manera, todas las funciones hiperbólicas y sus inversos pueden ser expresadas a través de funciones elementales sobre el campo $\mathbb{R}$.

14.2. Funciones especiales

En la conclusión del capítulo 9 se hace referencia a la existencia de dos perspectivas distintas a la que se tomó en esta investigación. La primera perspectiva nueva es la de las funciones elementales reales, que se utilizan para resolver el mismo problema que resuelven las funciones elementales aquí estudiadas, pero completamente dentro de los números reales. La segunda perspectiva nueva es la de funciones no elementales, las cuales surgen al integrar funciones elementales que no poseen una antiderivada elemental. En este anexo, se definirán las bases de ambas perspectivas.

14.2.1. Funciones elementales reales

En los artículos de Risch [18] y Bronstein [4] se discuten las funciones elementales reales. Entre ellas, se encuentran las funciones logarítmicas, exponenciales y algebraicas, las cuales se definieron en el capítulo 7. Sin embargo, hacen falta dos nuevas funciones, que permiten el uso de funciones trigonométricas y sus inversas sin necesidad del campo de los números complejos.

Definición 14.1 (Tangente)**:** Sea F un campo diferencial, y sea G una extensión diferencial de F. Sea $g \in G$ tal que existe $f \in F$ que cumple la ecuación diferencial

$$D(g) = (1 + g^2)D(f). \tag{14.11}$$

Entonces, se dice que g es una *tangente* sobre F. Esto se denota a través de $g = \tan(f)$.

La intuición detrás de esta definición proviene de notar que si $g = \tan(f)$, usualmente se esperaría que $D(g) = \sec^2(f)D(f)$. Pero $\sec^2(f) = 1 + \tan^2(f)$, que es el factor que aparece en la definición.

Definición 14.2 (Tangente inversa)**:** Sea F un campo diferencial, y sea G una extensión diferencial de F. Sea $g \in G$ tal que existe $f \in F$ que cumple la ecuación diferencial

$$D(g) = \frac{D(f)}{1 + f^2}. \tag{14.12}$$

Entonces, se dice que g es una *tangente inversa* sobre F, y se denota con $g = \tan^{-1}(f)$.

Es posible apreciar una similitud entre las funciones tangente y tangente inversa como la que existe entre las funciones logaritmo y exponencial. Esto se debe a que en ambos casos se está trabajando con funciones inversas, de manera que $g = \tan(f)$ si y solo si $f = \tan^{-1}(g)$, bajo una elección apropiada de los campos diferenciales.

A través de estas nuevas funciones, es posible adquirir todas las demás funciones trigonométricas y sus inversos. Para seno y coseno,

$$\sin(x) = \frac{2\tan\left(\frac{x}{2}\right)}{1 + \tan^2\left(\frac{x}{2}\right)}, \qquad \cos(x) = \frac{1 - \tan^2\left(\frac{x}{2}\right)}{1 + \tan^2\left(\frac{x}{2}\right)}. \tag{14.13}$$

Y para las tres restantes, los recíprocos son suficiente. Por otro lado, para las funciones trigonométricas inversas basta notar que

$$\sin^{-1}(x) = \tan^{-1}\left(\frac{x}{\sqrt{1 - x^2}}\right). \tag{14.14}$$

En cuanto a las funciones restantes, las ecuaciones 14.5 y 14.6 se encargan de su representación.

En este estudio, también es usual definir a la tangente hiperbólica y a su inversa de manera algebraica. Sin embargo, estas funciones ya están definidas en el anexo 14.1, específicamente en las ecuaciones 14.7 y 14.8. En ambas formulaciones es claro que los números complejos no son necesarios, por lo cual las tangentes hiperbólicas y sus inversos pueden verse como funciones reales dependientes de las exponenciales y los logaritmos. Lo mismo no es cierto sobre la tangente y la tangente inversa, pues estas solo dependen de las exponenciales y los logaritmos en el campo complejo. En $\mathbb{R}$, estas funciones son completamente independientes e irredundantes.

14.2.2. Algunas funciones no elementales

Al integrar ciertas funciones cuyas antiderivadas son no elementales, a menudo es posible notar que estas pueden ser expresadas a través de otras funciones no elementales más "simples". Este comportamiento puede observarse en el ejemplo 10.5,

$$\int \log(\log(x))\,\mathrm{d}x = x\log(\log(x)) - \mathrm{li}(x).$$

Aquí $\mathrm{li}(x) = \int \frac{1}{\log(x)}\,\mathrm{d}x$, la cual se demostró que es no elemental en el ejemplo 10.1. Esto ha incentivado el estudio de las funciones especiales para representar varias antiderivadas no elementales. En esta sección, se presentan definiciones de varias de estas funciones especiales, como surgen en los artículos de Baddoura [2] y de Cherry [5].

Definición 14.3 (Logaritmo integral)**:** Sea F un campo diferencial, y sea G una extensión diferencial de F. Sea $g \in G$ tal que existe $u \in F$ con $\log(u) \in F$ que cumple la ecuación diferencial

$$D(g) = \frac{D(u)}{\log(u)}. \tag{14.15}$$

Entonces, se dice que g es un *logaritmo integral* sobre F, y se denota con $g = \mathrm{li}(u)$.

La función logaritmo integral básica surge de tomar $u = x$. Otra función que resulta ser un logaritmo integral es la función exponencial integral $\mathrm{Ei}(x) = \int \frac{e^x}{x}\,\mathrm{d}x$, la cual es no-elemental según el ejemplo 10.13. Esto, a través de la función $u = e^x$. Así,

$$D(g) = \frac{D(e^x)}{\log(e^x)} = \frac{e^x}{x} \implies \mathrm{li}(e^x) = \int \frac{e^x}{x}\,\mathrm{d}x\,.$$

Aunque la notación es similar, no debe confundirse la función logaritmo integral con el dilogaritmo, presentado seguidamente.

Definición 14.4 (Dilogaritmo)**:** Sea F un campo diferencial, y sea G una extensión diferencial de F. Sea $g \in G$ tal que existe $u \in F$ que cumple la ecuación diferencial

$$D(g) = \frac{D(u)\log(1-u)}{u}. \tag{14.16}$$

Entonces, se dice que g es un *dilogaritmo* sobre F, y se denota por $g = \mathrm{Li}_2(u)$.

Tomando $u = 1 - e^x$ en la definición del dilogaritmo, se obtiene el caso del ejemplo 10.10 para los parámetros $n = 1$, $\alpha = -1$, y $\beta = -1$. Esto, pues se tendría

$$D(g) = \frac{D(1-e^x)\log(e^x)}{1-e^x} = \frac{-xe^x}{1-e^x} = \frac{-x}{-1+e^{-x}} \implies \mathrm{Li}_2(1-e^x) = \int \frac{x}{-1+e^{-x}}\,\mathrm{d}x\,.$$

Cabe resaltar que el dilogaritmo es el caso especial $s = 2$ de los polilogaritmos, que siguen la siguiente recursión integral:

$$\mathrm{Li}_s(z) = \int \frac{\mathrm{Li}_{s-1}(z)}{z}\,\mathrm{d}z\,.$$

El estudio de la integración simbólica en términos de polilogaritmos sigue en proceso, pero pueden encontrarse resultados parciales en el artículo de Hebisch [10], publicado en 2019.

Definición 14.5 (Función error)**:** Sea F un campo diferencial, y sea G una extensión diferencial de F. Sea $g \in G$ tal que existe $u \in F$ que cumple la ecuación diferencial

$$D(g) = \frac{2}{\sqrt{\pi}}\exp\left(-u^2\right)D(u). \tag{14.17}$$

Entonces, se dice que g es una *función error* sobre F, y se denota por $g = \mathrm{erf}(u)$.

Tomando $u = x$ en esta definición, se obtiene la integral del ejemplo 10.12. Esta es, sin lugar a dudas, una de las integrales no-elementales más útiles en la ciencia y tecnología.

Lista de símbolos

(a, b)	Máximo común divisor de a y b.
$\deg(f)$	Grado de la función polinómica f.
$\det(M)$	Determinante de la matriz M.
$\int f(x)\,\mathrm{d}x$	Integral de la función $f(x)$ con respecto a la variable x.
$\prod_{k=a}^{b} c_k$	Producto desde a hasta b de términos de la sucesión$\{c_k\}_{k\in\mathbb{Z}}$.
$\sum_{k=a}^{b} c_k$	Suma desde a hasta b de términos de la sucesión $\{c_k\}_{k\in\mathbb{Z}}$.
$\emptyset$	Conjunto vacío.
$\in$	Relación de pertenencia.
$\mathbb{C}$	Conjunto de números complejos.
$\mathbb{N}$	Conjunto de números naturales.
$\mathbb{Q}$	Conjunto de números racionales.
$\mathbb{R}$	Conjunto de números reales.
$\mathbb{Z}$	Conjunto de números enteros.
$\notin$	Relación de no pertenencia.
$\mathrm{res}_x(f, g)$	Resultante sobre el símbolo x de los polinomios f y g.
$\subseteq$	Relación de subconjunto.
$f : A \to B$	Función f con dominio en A y contradominio en B.
$K(x)$	Conjunto de funciones racionales con coeficientes en K sobre la variable x.
$K[x]$	Conjunto de polinomios con coeficientes en K sobre la variable x.
$p \mid q$	Relación p divide a q.
$p \nmid q$	Relación p no divide a q.